

**National HIV Behavioral Surveillance System:
Men Who Have Sex with Men – Round 3
(NHBS-MSM3)**

Model Surveillance Protocol



**Behavioral Surveillance Team
NCHSTP/DHAP-SE/BCSB**

Version Date: December 2010

Contents

1	Introduction.....	1-1
1.1	Purpose of the National HIV Behavioral Surveillance System.....	1-1
1.2	Timeline and Scope of Protocol.....	1-1
1.3	Collaborating Agencies.....	1-2
1.4	Responsibilities.....	1-3
1.5	Justification for NHBS-MSM3.....	1-3
1.6	Description of the Sample.....	1-4
1.7	General Approach	1-5
1.8	Objectives	1-5
1.9	Purpose and Use of the NHBS-MSM3 Surveillance Protocol.....	1-6
2	Formative Research Activities	2-1
2.1	Definition and Goals of Formative Research.....	2-1
2.2	Review of Secondary Data.....	2-2
2.3	Qualitative Data Collection.....	2-2
2.4	Garnering the Support of Community Stakeholders.....	2-4
2.5	Identification of Venues.....	2-5
2.6	Ongoing Formative Research	2-8

3	Data Collection	3-1
3.1	Data Collection Instruments	3-1
3.2	Translation of Data Collection Instruments	3-2
3.3	General Data Collection Procedures	3-2
3.4	Monitoring Data Collection	3-4
3.5	Training for Study Personnel	3-4
4	Sampling and Recruitment Methods	4-1
4.1	Overview.....	4-1
4.2	Monthly Recruitment Calendar.....	4-1
4.3	Recruitment Events.....	4-2
5	HIV Testing.....	5-1
5.1	Overview.....	5-1
5.2	Procedures and Methods.....	5-1
5.3	Data Management	5-5
6	Data Management.....	6-1
6.1	Overview.....	6-1
6.2	Data Configuration.....	6-1
6.3	NHBS-MSM3 Analysis File.....	6-2
7	Data Analysis and Dissemination	7-1
7.1	Data Analysis and Dissemination	7-1
7.2	Limitations and Potential Biases.....	7-1

8	Data Security and Confidentiality.....	8-1
8.1	HIV/AIDS Surveillance Assurance of Confidentiality.....	8-1
8.2	Written Data Security Policy	8-1
8.3	Security and Confidentiality Requirements	8-1
8.4	Breaches in Data Security Procedures	8-5
9	Human Subjects Considerations.....	9-1
9.1	Institutional Review Board Approval	9-1
9.2	Potential Risks and Anticipated Benefits.....	9-1
9.3	Voluntary Participation	9-2
9.4	Vulnerable Populations	9-3
9.5	Informed Consent Process	9-3
9.6	Age of Participants.....	9-3
9.7	Anonymity and Privacy Protection.....	9-4
9.8	Reimbursement for Time and Effort.....	9-5
9.9	Adverse Events	9-6
10	References	10-1

Appendices

<i>A</i>	<i>Model Key Informant Interview Consent</i>	<i>A-1</i>
<i>B</i>	<i>Model Community Key Informant Consent Form</i>	<i>B-1</i>
<i>C</i>	<i>Model Focus Group Consent</i>	<i>C-1</i>
<i>D</i>	<i>Intercept Form.....</i>	<i>D-1</i>
<i>E</i>	<i>Data Collection Instrument</i>	<i>E-1</i>
<i>F</i>	<i>Model Consent Form</i>	<i>F-1</i>
<i>G</i>	<i>Improved Referral to Care for NHBS-MSM3 Participants Using a Rapid Test Algorithm</i>	<i>G-1</i>
<i>H</i>	<i>Telephone Results</i>	<i>H-1</i>
<i>I</i>	<i>FDA Letter</i>	<i>I-1</i>
<i>J</i>	<i>HIV Test Log</i>	<i>J-1</i>
<i>K</i>	<i>Assurance of Confidentiality for HIV/AIDS Data.....</i>	<i>K-1</i>
<i>L</i>	<i>Guidelines for HIV/AIDS Surveillance.....</i>	<i>L-1</i>
<i>M</i>	<i>Model Waiver of Documentation of Informed Consent.....</i>	<i>M-1</i>
<i>N</i>	<i>Required Elements of Informed Consent</i>	<i>N-1</i>

1.1 Purpose of the National HIV Behavioral Surveillance System (NHBS)

Based on a June 1999 review of national HIV prevention programs, CDC's Advisory Committee for HIV and STD Prevention and other external experts called for the development of a national plan for HIV/AIDS prevention. In 2000, CDC, in collaboration with representatives from state and local health departments, academic institutions, and clinical and prevention organizations, initiated a strategic planning process that culminated in the development of CDC's HIV Prevention Strategic Plan Through 2005 (CDC, 2001). As part of this plan, four national goals were identified to reduce the annual number of new HIV infections in the United States by half. One of these goals was to strengthen the national capacity to monitor the HIV epidemic to better direct and evaluate prevention efforts. In 2002, as an initial step toward meeting this goal, CDC awarded supplemental funds to state and local health departments to develop and implement a surveillance system to monitor behaviors that place people at risk for HIV infection (Lansky *et al.*, 2007). This system is called the National HIV Behavioral Surveillance System (NHBS) (Gallagher *et al.*, 2007).

NHBS was developed to help state and local health departments establish and maintain a surveillance system to monitor selected behaviors and prevention services among groups at highest risk for HIV infection. Findings from NHBS are used to enhance the understanding of HIV risk and testing behaviors in these groups, and to develop and evaluate HIV prevention programs that provide services to them. Within each participating Metropolitan Statistical Area (MSA), data are collected within the major city or HIV epicenter. Depending on the cycle and sampling method, other areas within the MSA may also be targeted for data collection.

NHBS activities are implemented in rounds composed of three cycles. The first cycle of each round focuses on men who have sex with men (MSM), the second cycle focuses on injecting drug users (IDU), and the third, on heterosexuals at increased risk of HIV infection (HET). These cycles are repeated in rounds so that data are collected from each risk group every three years. Cycles are referred to by the group of interest (NHBS-MSM, NHBS-IDU, and NHBS-HET), and the round of data collection is indicated by a number following the group of interest (e.g., NHBS-MSM1, NHBS-MSM2, etc).

1.2 Timeline and Scope of Protocol

In the first round of NHBS, data collection for NHBS-MSM1 occurred December 2003 – December 2004, data collection for NHBS-IDU1 occurred January 2005 – December 2005, and data collection for NHBS-HET1 occurred January 2006 – October 2007; and in the second round

of NHBS, data collection for NHBS-MSM2 occurred January 2008 – December 2008, data collection for NHBS-IDU2 occurred January 2009 – December 2009, and data collection for NHBS-HET2 started in January 2010 and will conclude in December 2010.

The third round of NHBS is scheduled to begin with NHBS-MSM3 in January 2011. NHBS-IDU3 will be conducted in 2012 and NHBS-HET3 in 2013. The activities described in this protocol are just for NHBS-MSM3; activities for NHBS-IDU3 and NHBS-HET3 will be described in future protocols.

1.3 Collaborating Agencies

The third round of NHBS begins in January 2011 under a new program announcement (PS-11-001). Participation in NHBS is limited to 6 city health departments independently funded by the Division of HIV/AIDS, CDC and 14 state health departments with jurisdiction over specific MSAs or Divisions within MSAs (see <http://www.census.gov/population/www/estimates/metrodef.html> for definitions of MSAs and Divisions).

For the third round of NHBS, CDC will collaborate with the following independently-funded city health departments: Chicago Division (Chicago MSA); Houston MSA; Los Angeles Division (Los Angeles MSA); New York Division (New York City MSA); Philadelphia Division (Philadelphia MSA); and San Francisco Division (San Francisco MSA); as well as the MSAs/Divisions under the jurisdiction of the following state health departments listed in brackets: San Diego MSA [California]; Denver MSA [Colorado]; Washington Division, Washington DC MSA [Washington DC]; Miami Division, Miami MSA [Florida]; Atlanta MSA [Georgia]; New Orleans MSA [Louisiana]; Boston Division, Boston MSA [Massachusetts]; Baltimore MSA [Maryland]; Detroit MSA [Michigan]; Nassau Division, New York MSA [New York]; Newark Division, New York MSA [New Jersey]; San Juan MSA [Puerto Rico]; Dallas Division, Dallas MSA [Texas]; and Seattle Division, Seattle MSA [Washington]. These grantees are referred to as “project sites” throughout this protocol.

Participation in NHBS is limited to ensure that the behavioral surveillance system covers geographic areas of the United States where the impact of the HIV epidemic is greatest. These 20 MSAs/Divisions represent the majority of all persons living with AIDS in large MSAs (population \geq 500,000) in the United States at the end of 2006 (CDC unpublished data). Participating health departments will be supported only within the MSA or Division listed and only within the geographic bounds of the funded entity (where MSAs extend beyond the jurisdiction of the eligible state or city health department). Where it would be impractical to conduct NHBS in the entire MSA or Division, venues and recruitment activities should be limited to the geographic area (e.g., city, county, or health district) within the MSA or Division with the highest HIV/AIDS morbidity. On the other hand, in order to preserve the integrity of the sampling method, venues and recruitment activities may be extended to geographic areas adjacent to the MSA or Division if HIV/AIDS morbidity in those areas is high and CDC has granted approval.

1.4 Responsibilities

The CDC investigators are principally responsible for writing the protocol and supporting appendices and will provide technical assistance to the local project sites during implementation. The local NHBS investigators will 1) assist with the creation of the protocol, 2) conduct the project using the methods described, and 3) submit data to CDC in a timely manner.

1.5 Justification for NHBS-MSM3

The HIV epidemic has disproportionately affected MSM. In the United States, just over half the persons living with HIV are MSM (CDC, 2008b), and 57% of all new HIV infections occur in MSM (Hall *et al.*, 2008). Moreover, MSM are the only risk group in the United States in which the number of new HIV diagnoses is increasing (CDC, 2008a). NHBS and other studies have found that rates of HIV infection among MSM remain persistently high, especially among racial and ethnic minority MSM, and that many HIV-infected MSM are unaware of their infections (Valleroy *et al.*, 2000; MacKellar *et al.*, 2005; CDC, 2005; CDC, 2010). These studies have also shown high levels of sexual and drug-use risk behavior (Valleroy *et al.*, 2000; MacKellar *et al.*, 2005; CDC, 2006).

NHBS-MSM3 will provide data on the sexual and drug-use risk behaviors that put MSM at risk for HIV infection, as well as provide data on their use of HIV prevention services. These data will provide valuable information for evaluating and guiding national and local HIV prevention efforts. NHBS-MSM3 data may be used by public health officials and researchers to identify HIV prevention needs, allocate prevention resources, and develop and improve prevention programs that target the MSM community. As a result of this survey, localities may obtain, allocate, or shift HIV prevention resources to the MSM community or to at-risk MSM sub-populations.

Although HIV behavioral surveillance data cannot be used to evaluate the efficacy of specific interventions, they are important for evaluating whether HIV prevention efforts are reaching at-risk populations within a community and whether these efforts meet national and local prevention goals. The ongoing and systematic collection and analysis of data is needed to identify baseline risk behaviors and prevention service utilization, as well as to measure progress toward meeting prevention goals. In addition, NHBS-MSM3 will provide information on the types of local HIV prevention programs accessed by MSM and the types of venues frequented by them. If some types of venues have attendees with significantly higher levels of risk behavior or rates of HIV infection, prevention programs can target these venues for outreach and services.

At the individual level, NHBS-MSM3 participants may benefit directly from HIV prevention counseling, knowledge of their HIV status, and referrals for additional HIV risk information and care. HIV-positive participants who return for their test results will be counseled and referred for treatment and case management services.

1.6 Description of the Sample

The target sample size for each project site is 500 completed interviews with eligible men who report having had sex with another man in the past 12 months. Across the 20 participating project sites, this would result in a combined sample size of 10,000 eligible MSM respondents.

1.6a Participant inclusion criteria

The criteria for participants to enroll in NHBS-MSM3 are that they:

- have not previously participated in NHBS-MSM3,
- are at least 18 years of age,
- live in the participating MSA or Division,
- are male,
- ever had oral or anal sex with another man,
and
- are able to complete the survey in English or Spanish.

A screener will be used to assess whether a respondent meets these eligibility criteria.

Activities that are part of NHBS-MSM3 include the eligibility screener, the survey, and an optional HIV test. Participants will receive a small stipend for participation in NHBS-MSM3 activities. The reimbursement amounts are determined locally by the NHBS-MSM3 project sites, and are based on previous experience with NHBS cycles or other similar studies. The reimbursement includes compensation for the survey and for taking an HIV test. The average amount of these reimbursements, based on compensation paid by similar studies in these cities, is \$25 for the survey and \$25 for the HIV test.

1.6b Participant exclusion criteria

Respondents are excluded from participating in NHBS-MSM3 if they:

- have previously participated in NHBS-MSM3,
- are less than 18 years of age,
- do not live in the participating MSA or Division,
- are not male,
- never had oral or anal sex with another man,
or
- are not able to complete the survey in English or Spanish.

NHBS is a surveillance system of the HIV risk behaviors of adults in the United States, and the methods used in NHBS-MSM3 are designed to recruit an adult population. Surveillance systems, such as the Youth Risk Behavior Surveillance System (YRBSS) are more appropriate to understand the risk behaviors of minors in the United States (CDC 2008c).

1.7 General Approach

NHBS-MSM is a repeated, cross-sectional survey of men who attend MSM-identified venues within local communities. The survey uses venue-based sampling, a method that has proven successful in obtaining large and diverse samples of MSM (MacKellar *et al.*, 1996; Diaz *et al.*, 2001; Muhib *et al.*, 2001; Stueve *et al.*, 2001; CDC, 2006; MacKellar *et al.*, 2007). Survey methods can be categorized into three principal activities. In the first activity, staff conduct formative research to prepare for sampling and recruitment by reviewing scientific, prevention, and commercial literature and interviewing persons knowledgeable about MSM and HIV prevention services. The objectives of these investigations are to construct an initial “universe” of MSM venues, to identify potential sampling and recruitment barriers, and to help construct prevention service measures for the survey. In the second activity, staff will assess the venues and day-time periods on the initial “universe” to determine which have a sufficient number of eligible MSM for conducting NHBS-MSM3 recruitment. These venues and day-time periods will then be included on the monthly sampling frames used to randomly select venues and day-time periods for recruiting participants. In the third activity, men are recruited to participate in NHBS-MSM3 at randomly selected venues during randomly selected day-time periods. At these recruitment events, staff count venue attendees, approach men to ask them to participate in the survey, interview eligible men, and offer HIV tests. Although the three activities are initially performed in sequence, sampling frames are continually updated throughout the project cycle.

1.8 Objectives

1.8a NHBS objectives

The objectives for NHBS apply to the data collected in all three project cycles: NHBS-MSM, NHBS-IDU, and NHBS-HET. The NHBS objectives are designed to better characterize those populations at high risk of HIV infection. They are as follows:

Risk Behaviors

- Assess the prevalence of and trends in risk behaviors, including:
 - sexual risk behaviors
 - drug-use risk behaviors

HIV Testing Behaviors

- Assess the prevalence of and trends in HIV testing behaviors.

Prevention

- Assess the exposure to and use of prevention services.
- Assess the impact of prevention services on behavior.
- Identify gaps in prevention services and missed opportunities for prevention interventions.

Seroprevalence

- Assess the prevalence of and trends in HIV infection.
- Assess behaviors associated with HIV infection.

1.9 Purpose and Use of the NHBS-MSM3 Surveillance Protocol

A protocol describes the methods that must be followed to conduct a project in a standardized manner. It also provides historical information about project development and design. A standardized protocol is essential for a multi-site project like NHBS; it ensures comparability of data across sites, thereby allowing the data to be aggregated in a single national dataset.

This protocol describes the activities that NHBS project sites will conduct for the NHBS-MSM3 cycle. The chapters include formative research activities (Chapter 2), data collection procedures and instruments (Chapter 3), sampling and recruitment methods (Chapter 4), HIV testing procedures (Chapter 5), data management (Chapter 6), plans for data analysis and dissemination (Chapter 7), data security and confidentiality guidelines (Chapter 8), human subjects considerations (Chapter 9), and references (Chapter 10).

2.1 Definition and Goals of Formative Research

Formative research is the process by which researchers or public health practitioners define the community of interest, ways of accessing that community, and the attributes of the community relevant to the specific public health issue (Higgins et al., 1996; Ulin et al., 2005). The purpose of NHBS formative research is to collect information to help NHBS project sites tailor the implementation of NHBS-MSM3 to their local setting. NHBS-MSM3 formative research activities are designed to help project sites: (1) describe the characteristics of MSM in the MSA; (2) gain an understanding of the context of HIV risk behavior among MSM locally; (3) garner the support of community stakeholders for the NHBS-MSM3 behavioral survey; (4) identify venues attended by MSM; (5) assess the suitability of these venues for recruiting participants and conducting surveillance activities; (6) develop questions of local interest for HIV prevention among MSM; and (7) monitor the on-going implementation of NHBS-MSM3.

Formative research activities are completed over a period of approximately 3 months that precedes the implementation of surveillance activities. All NHBS project sites are strongly encouraged to hire a local ethnographer to guide the collection, analysis, and interpretation of qualitative formative research data.

2.1a Goals of formative research

The major goals of the formative research are to:

- Ensure that an adequate number of eligible respondents are recruited and interviewed during NHBS-MSM3 and that the resulting sample reflects the broader MSM community;
- Identify appropriate venues and venue day-time periods for sampling;
- Obtain information about operational issues (e.g. staffing, logistics, and scheduling of recruitment events) that need to be considered prior to and during the data collection period.

There are a number of additional benefits to formative research. Formative research can provide information on the sociocultural context of HIV risk behavior among MSM in the local area. Conducting formative research will be beneficial in identifying community and neighborhood organizations that serve MSM; key individuals who are knowledgeable about and have access to MSM in the community; social networks among MSM; and barriers to NHBS-MSM3 participation.

A number of methods should be employed in order for sites to meet the formative research goals. These methods include a secondary data review, key informant interviews, community key informant interviews, focus group interviews, observations, and street intercept surveys.

A key feature of the NHBS formative research component is that it is an iterative process: knowledge about the study population of interest builds on information collected during each of the formative research activities mentioned above. This on-going processing of formative research helps project staff identify gaps in knowledge and determine if there is a need to collect additional information. When necessary, initial assumptions or conclusions are revised.

Upon completion of their formative research activities, project sites compile their findings into a series of short reports which are sent to their CDC Project Officer. These reports serve as the basis from which project sites, in consultation with CDC, communicate the goals of NHBS-MSM3 to their local communities and tailor the implementation of the project to ensure its acceptability.

2.2 Review of Secondary Data

The primary purpose of the secondary data review is to establish a foundation of information on populations of interest within the designated MSA or Division. Existing (published and unpublished) data are reviewed to:

- Describe the general characteristics of local MSM (e.g., age, race/ethnic group, geographic location, other risk behaviors, etc.)
- Characterize the local HIV/AIDS epidemic among MSM
- Compile a list of community stakeholders, health department staff, and key informants to be contacted for formative research interviews
- Identify organizations providing HIV prevention services to MSM
- Develop a list of venues frequented by MSM
- Identify gaps in knowledge about local MSM

Secondary data sources include surveillance data on HIV/AIDS, hepatitis, and other sexually transmitted diseases; HIV epidemiological profiles; HIV prevention plans; HIV counseling and testing data; data from community-based studies of MSM; and other print and on-line media targeting the local gay community.

2.3 Qualitative Data Collection

NHBS-MSM3 formative research activities include the collection of qualitative data using an array of methods common to many qualitative and ethnographic studies of health: key informant

interviews, focus group interviews, brief intercept surveys, and observation (Kreuger and Casey 2000; Lambert et al. 1995; Power 2002; Schensul and LeCompte 2002; Scrimshaw et al. 1991; Stimson et al. 2002; Needle et al. 2002; Trotter et al. 2001). These qualitative methods are briefly described here.

2.3a Interviews with key informants

Key informants serve as "cultural experts," offering insight into the context of HIV risk behavior among MSM locally, as well as the types of venues where MSM can be recruited. Although good key informants may not know everything there is to know about MSM in the MSA, they should be able to contribute to the understanding of how best to approach potential participants and identify problems that NHBS-MSM3 staff may encounter in the field. A diverse group of key informants should be interviewed to accurately reflect the characteristics of the MSM locally (Schensul et al. 1999). Examples of key informants include: gay community leaders, owners of local businesses that cater to MSM, persons doing outreach work among MSM, members of the local MSM community, and researchers familiar with local MSM.

Interviews with key informants will be unstructured and open-ended, allowing for detailed and in-depth discussions of issues. Information collected through key informant interviews can be exploratory in nature (e.g., the locations where MSM meet and socialize, types of drugs used by MSM, and the demographic characteristics of local MSM) or focused on particular topics (e.g., the best days and times to recruit at venues and barriers to recruitment). Appendix A contains a model consent form for key informant interviews where compensation for participation is not appropriate, such as with health department officials, venue owners, business and community leaders, and others for whom the dissemination of information on local neighborhoods to researchers and public health workers is not outside of the scope of their normal duties. Appendix B contains a model consent form for members of the local MSM community who would not be able contribute information about local MSM without being compensated for their time and effort. These forms should only be modified to meet local IRB requirements. Consent to participate will be obtained orally.

2.3b Focus groups

Focus groups are semi-structured interviews conducted with several individuals at a time, under the direction of a moderator (Kreuger and Casey 2000). This interview format can provide quick information about general topics of interest (e.g., drug use among local MSM, means of recruiting non gay-identified MSM to participate in the survey, and the identification of MSM community stakeholders and local leaders) or specific information on issues about which little is known (e.g. where local MSM go to look for sex and how the NHBS-MSM3 survey should be marketed locally). Information collected through these semi-structured interviews may be used to validate findings from the secondary data review or to explore issues that were raised by key informants or were observed by staff in the field.

Participants in focus group discussions should be recruited from within the MSA. Focus group

participants may include community stakeholders regardless of their sexual identity (e.g., owners of local business that cater to MSM, gay community leaders, and staff in organizations that serve either local MSM populations or the gay community) and groups of hard-to-reach MSM (e.g., racial or ethnic minority MSM and non-gay identified MSM). To protect the anonymity of the persons in the focus groups, focus groups cannot be video- or audio-taped.

Focus group content and procedures are determined locally. Each NHBS-MSM3 project site will need to follow their local requirements regarding informed consent procedures for focus group participants. Appendix C contains a model consent form; this form should only be modified to meet local IRB requirements. Consent to participate will be obtained orally.

2.3c Observations

Unlike the information collected from key informant or focus group interviews, observation relies solely on what is seen by the researcher (Schensul et al. 1999; Trotter et al. 2001). Being there and observing what is happening "on-the-ground" can provide staff with important insight into the behavior of local MSM at particular locations or within particular venues. Observations of the clientele at potential MSM venues, as well as the venue layout, will provide important information on venue attendance, the characteristics of venue attendees, and the logistics and safety of conducting surveillance activities at the venue.

2.3d Street intercept surveys

A street intercept survey involves asking individuals in key locations (e.g., men near or in venues frequented by MSM) about topics relevant to NHBS-MSM3. The survey is very brief (5 minutes maximum) and is typically conducted where the person is intercepted. Brief intercept surveys are an easy and useful method of soliciting the spontaneous input of community members. They can be used to identify venues where MSM can be recruited to participate in NHBS-MSM3 and to determine when the best days and times would be for recruiting participants. Once potential venues have been identified, additional intercept surveys can be conducted with venue patrons to assess their eligibility and willingness to participate in the project. In addition, street intercept surveys can be used to disseminate information about NHBS-MSM3 among local MSM; ask MSM about perceived barriers to the project; and garner support of MSM in the community to participate in NHBS-MSM3 if recruited during data collection activities. The street intercept survey is not intended to obtain detailed information about the target population; rather, it is a method that field staff can use to assess the support for NHBS-MSM3 in the community and to distribute information about the project to MSM and other stakeholders.

2.4 Garnering the Support of Community Stakeholders

The support of stakeholders in the communities where NHBS-MSM3 will be conducted is key to ensuring the acceptability of NHBS-MSM3 by both participants and venue owners. Community

stakeholders will come from different backgrounds, affiliations, and interests. Key stakeholders for NHBS-MSM3 may include individuals from the following groups or organizations:

- Community groups and social organizations that serve MSM
- Community-based organizations that target MSM
- Owners of businesses that cater to MSM
- Gay community leaders
- Municipal liaisons with the gay community (e.g., liaisons from the mayor's office or the police department)

A number of methods can be used to identify community stakeholders. These include, but are not limited to, the following:

- Abstracting names of stakeholders from print and on-line media data sources,
- Eliciting names of stakeholders from key informants or focus group participants,
- Requesting a list of potential community stakeholders during meetings with health department representatives when eliciting their input on NHBS-MSM3,
- Asking about stakeholders during street intercepts at local events targeting MSM, and
- Observing persons at public meetings about issues affecting the gay community or MSM.

Once the key stakeholders have been identified, the formative research field staff should hold a series of formal or informal meetings with them. The goal of these meetings is to provide community stakeholders with opportunities to learn more about NHBS-MSM3 and to identify any potential barriers to implementing NHBS-MSM3, both logistically and in terms of community acceptance. Stakeholders will also have the opportunity to provide input on the development of questions of local interest.

2.5 Identification of Venues

NHBS-MSM3 project sites will be required to conduct a number of activities to identify venues. These include identification of venues within the MSA, qualitative data collection such as interviews with key informants, focus group interviews, and observation (to collect information on these enumerated venues and to describe the characteristics of those who frequent these venues), and type I and type II enumeration of venues.

2.5a Venue definition

A venue is an area, location, or building where men can be approached and recruited to participate in the NHBS-MSM3 survey. Venues for consideration for NHBS-MSM3 are found

within the MSA and are defined as public or private locations that are attended by men for purposes *other* than receiving medical or mental healthcare, social services, or HIV/STD diagnostic testing or prevention services. Support groups for HIV-infected persons and clinical or other settings that routinely provide medical care, mental healthcare, social services, or HIV/STD diagnostic or other prevention services are ineligible for consideration as venues. Venues may include bars, dance clubs, retail businesses, cafes and restaurants, health clubs, social and religious organizations, adult bookstores and bathhouses, high-traffic street locations, parks, beaches, and special events such as gay pride festivals, raves, and circuit parties. These venues may be considered even though some healthcare, HIV/STD diagnostic, or prevention services may be available on site (e.g., HIV testing services provided in some bathhouses).

2.5b Methods

Venue identification involves the steps described below. These steps result in a universe of venues which will be verified with key informant and focus group participants. Project staff will use the venue universe to conduct observations and brief interviews of venue attendees. After completing all of these activities, a list of viable venues will be finalized and used to create the monthly sampling frames (see Chapter 4).

Identify all venues

The first step in the venue identification process is to identify all potential venues within the MSA where MSM can be interviewed. During the identification process, NHBS-MSM3 project staff should be liberal with their assessments; that is, do not exclude any potential venues at this point. However, potential street locations should be limited to areas where there is high foot traffic. “High traffic street locations” refer to corners or other areas of sidewalks that are well-attended (i.e., get a lot of foot traffic) and that are not associated with any one particular type of venue such as bars, cafés, dance clubs, etc. “High traffic street locations” are not a substitute for individual venues. If a street has a substantial traffic flow of MSM because several potential venues are located on the street (e.g. bars, clubs, cafes), the individual venues themselves should be identified as potential venues rather than identifying the street as a “high traffic street location.” For this reason, high-traffic street locations should be a small proportion of all venues identified.

To verify the universe of eligible venues, staff should review all local publications that advertise venues and interview as many persons as practical from the community that are knowledgeable about venues within the MSA. Interviews may be conducted with community members, staff of health department prevention programs, community-based organizations, community leaders, and venue owners, managers, workers, and patrons.

Determine suitability of venues

The next step in the venue identification process is to identify people who can provide insight into the suitability of the enumerated venues. This information can be collected from multiple sources in the community, using a combination of qualitative methods described above in section

2.3. Issues like safety of the venue, the composition of participants that go to that venue, days and times of highest attendance at the venue, and other comments can be elicited. Interviewees are first asked to review the venue universe and add other venues that are attended by MSM. They will then be asked to identify the days and times (day-time periods) when these venues are most heavily attended by MSM. The updated list of venues and associated high-attendance day-time periods will then be shown to the next interviewee who will be asked to add to the list. This process is repeated until additional venues and associated day-time periods are no longer elicited. Secondly, project staff must ensure that MSM who represent important demographic and social subpopulations review updated lists to ensure all eligible venues and day-time periods have been identified. To help ensure the representativeness of eligible venues and day-time periods, interviews should be conducted with MSM who are of various racial and ethnic backgrounds and ages.

Interviews with key informants should also elicit, by venue, the socio-demographic characteristics of patrons as well as potential barriers to recruiting and interviewing men. Assessing socio-demographic characteristics of venue patrons will enable NHBS-MSM3 project staff to monitor these distributions and help ensure the elicitation of venues that are attended by important subpopulations. Identifying potential recruitment and interview barriers will help staff to further assess, clarify, and prevent or minimize sampling barriers. Potential barriers that should be assessed include structural, management, safety, parking (if interview vans are used), and competing outreach activities.

2.5c Assessment of venue attendees

Once venues are identified it is necessary to determine if a sufficient number of eligible people attend the venue. This involves collaborating with the venue owners or managers, as well as other prevention programs that may be working in the same venues. Two types of enumerations may be conducted at those venues with unknown attendance patterns.

Collaboration with venue owners/managers

NHBS-MSM project staff will need to obtain the approval of venue owners or managers before conducting type 1 or type 2 enumerations or observations. Approval is necessary to conduct sampling events just outside of or within these establishments. In meeting with venue owners or managers, project staff should emphasize individual and community benefits of NHBS-MSM3 and that sampling activities will be conducted in ways to minimize burden on venue management and patrons.

Type 1 and 2 enumerations

Type 1 enumerations are conducted by one person and are simple counts of people attending venues during 30- to 60-minute periods. Type 1 is the optimal enumeration method when staff believe that people attending the venue are predominately MSM. Type 2 enumerations are conducted with two project staff who count and briefly interview men on their sexual behavior and eligibility for NHBS-MSM3. Type 2 enumeration provides attendance estimates of eligible

MSM and is the optimal method when staff suspect that venues are attended by a large number of people who only have had sex with someone of the opposite sex or who are too young to be eligible for NHBS.

Venue observations

During type 1 and 2 enumerations, staff should also conduct observations. The purpose of observations is to make note of key characteristics about the venue and venue attendees that may affect venue selection and future recruitment activities. These include: 1) activities that are occurring at the venue during specific days and times, 2) the safety and feasibility of conducting interviews at the venue, 3) locations where recruitment should be conducted (inside the venue, near the entrance, etc), and 4) characteristics of venue attendees (age, race, gender, etc).

Collaboration with other organizations

Project staff will also need to collaborate with organizations that conduct outreach prevention or research activities at identified venues. Project staff should first interview health department HIV/STD prevention staff and community informants about the organizations that are known to conduct these activities and where and when they are conducted. Project staff should then inform managers of these organizations about NHBS-MSM3 and the need to collaborate. As part of collaborative agreements, monthly outreach calendars should be shared between organizations to prevent activities that occur at the same place, date, and time.

2.6 Ongoing Formative Research

NHBS-MSM3 project sites will also conduct ongoing formative research once data collection starts to monitor the quality of the data collection process. Project sites will use a combination of qualitative and quantitative methods to monitor enrollment rates, suitability of venues for recruitment, potential concerns about the percent of eligible respondents at venues, demographic characteristics of the sample, and other relevant indicators of data quality. Ongoing formative research will also monitor whether new venues have opened or started attracting a population of MSM during the data collection period and whether these venues would be acceptable for NHBS-MSM3 recruitment.

Ongoing formative research may be conducted by field supervisors and interviewers by observing the behaviors of participants before and during the interview, as well as by monitoring data collection. As a result of findings from ongoing formative research, project sites may need to make modifications to their operations, as approved by their CDC Project Officer.

3.1 Data Collection Instruments

3.1a Intercept Form

Each recruiter will use the Intercept Form (Appendix D) during recruitment events to record intercept data on men who are counted and approached. The two questions asked of potential participants during the intercept are whether he has already been asked to participate in NHBS-MSM3 and whether he previously participated in NHBS-MSM3.

3.1b Eligibility screener

NHBS-MSM3 participants screened for eligibility before participation in the NHBS-MSM3 survey. Eligibility screening makes efficient use of staff and respondent time by quickly identifying those who are eligible and ineligible. Eligible individuals:

- Have not previously completed an interview for NHBS-MSM3;
- Are at least 18 years of age;
- Live in the participating MSA;
- Are male (not transgender);
- Ever had oral or anal sex with another male;
- *and*
- Are able to complete the interview in English or Spanish.

Screening for eligibility is important for ensuring that all NHBS-MSM3 participants meet the same eligibility criteria for participation, allowing for comparison across all NHBS project sites.

3.1c Questionnaire

Questionnaire components

The NHBS Round 3 questionnaire consists of two components. The first is a standardized set of core questions, some of which are asked only during the relevant cycle (MSM, IDU, or HET). The NHBS questionnaire is a single document (Appendix E). The computerized version of the questionnaire will be set for each cycle so that interviewers can only administer the appropriate cycle-specific version. The NHBS questionnaire is approved by OMB (Round 3 control number pending). In addition to the core questions, participating NHBS-MSM3 project sites may develop and add questions that address topics of local interest.

Core Questions. The core questions will be used by all participating NHBS-MSM3 project sites and will provide data that will be used for comparisons of MSM risk behaviors and HIV testing behaviors between the MSAs. The core questionnaire covers the following areas:

- Demographics
- Sexual behaviors
- Alcohol and drug use history
- HIV testing experiences
- Health conditions
- Assessment of exposure to prevention activities

Local Use Questions. Project sites may include additional questions on topics of local interest. Local use questions should not exceed 10 minutes for administration.

Development of the questionnaire

Development of the NHBS questionnaire is a collaborative process between participating NHBS project sites and CDC. Prior to development of the NHBS Round 3 questionnaire, NHBS project site staff and the Behavioral Surveillance Team evaluated the Round 2 questionnaire and data. In addition, BST reviewed reports of cognitive testing previously conducted for NHBS items. Questions were evaluated and revised as necessary, and several new questions were identified for inclusion in order to incorporate the need for data on emerging issues. Select items were also reviewed by subject matter experts. All decisions regarding changes to the questionnaire were made to optimize data quality, provide consistent measurement over time for key NHBS indicators, and reduce respondent burden.

3.2 Translation of Data Collection Instruments

All NHBS-MSM3 data collection instruments that involve questions asked directly of participants will be available in English and Spanish. Formatting and appearance of these instruments are the same in both languages. CDC is responsible for translating the eligibility screener, core questionnaire, and other standardized or model materials (e.g., model consent script) into Spanish. Translation of the data collection instruments by a single source ensures consistency across all states and populations. Translation into Spanish of the data collection instrument (except local questions) by other sources is prohibited. Local areas are responsible for translating local questions into Spanish. No other languages will be used for NHBS and the use of translators is prohibited.

3.3 General Data Collection Procedures

Data will be collected in a number of steps for NHBS-MSM3. These are described below. The data collection instrument application is developed for use in the handheld computer-assisted personal interview (HAPI) program and will be administered by the interviewers.

Step 1: Approach

Potential participants will be approached and asked about their interest in participating in NHBS-MSM3 and whether they have previously participated. Intercept information is recorded on the Intercept Form (Appendix D).

Step 2: Eligibility assessment

Potential participants will be assessed using the eligibility screener (Appendix E). The eligibility screener is administered using a HAPI program on a handheld computer. An algorithm, programmed into the computer, is used to determine which participants are eligible. The HAPI program will automatically end after the eligibility screener is completed if the respondent is not eligible.

Step 3: Obtaining consent

Interviewers will provide informed consent information (Appendix F) to the respondents and address any questions. Consent to participate will be obtained orally. Interviewers will check a box on the handheld computer indicating whether consent was obtained. The HAPI program will automatically end if the respondent does not agree to participate in the survey. Respondents may consent to the survey and any of the following: survey, HIV testing, other tests offered locally (e.g., hepatitis, STD), and if applicable, blood storage. Participants must consent to the survey to be eligible for the other components; however, if participants do not consent to the survey but still wish to receive an HIV test or other tests, project staff in each NHBS site will provide referrals and information in order for the person to access these resources.

Step 4: Core questionnaire and local questions

Eligible participants who provide consent will be administered the NHBS-MSM3 questionnaire (Appendix E). The local questions will be launched automatically at the end of the core survey; these questions are also administered to respondents by the interviewer.

Step 5: HIV testing

HIV testing procedures and the information recorded in the HIV testing log do not require that questions be asked of the participants. See Chapter 5 for more details on testing procedures.

Step 6: Participation incentives

Participants will receive a small stipend for participation in NHBS-MSM3 activities. The reimbursement amounts are determined locally by the NHBS-MSM3 project sites, and are based on investigators' previous experience with NHBS cycles or other similar studies. The reimbursement includes compensation for the survey (approximately \$25) and for taking an HIV

test (approximately \$25). If local regulations prohibit cash disbursement, equivalent reimbursement may be offered (e.g., gift certificates, tokens for public transportation).

Local areas may have requirements about documenting payment of incentives. This should be done in accordance with requirements for maintaining anonymity (see Chapter 9).

3.4 Monitoring Data Collection

All interview data are vulnerable to bias from variability in the way respondents are sampled and in the way interviews are conducted. This bias may arise from variability between interviewers or from variability between interviews conducted by a single interviewer. To prevent these biases, and to ensure that proper procedures are followed, monitoring procedures should be implemented to assess the consistency and quality of NHBS data collection activities.

The NHBS-MSM3 field supervisor or another project manager should periodically monitor each staff member as they approach and recruit potential participants, conduct the eligibility screener, obtain informed consent, and administer the NHBS-MSM3 questionnaire. Feedback on their performance – areas of proficiency as well as areas for improvement – should be given shortly after observations are conducted. Supervisors should monitor 10% of interviews administered by each interviewer.

3.5 Training for Study Personnel

All NHBS-MSM3 personnel will be appropriately trained to conduct surveillance activities. CDC will hold Field Operations training for Project Coordinators and Field Supervisors covering topics including: proper survey administration; required elements of informed consent; techniques for monitoring interviewers and staff; and instructions for creating a local training for interviewers and other project staff. Representatives from the Data Coordinating Center, or DCC (Chapter 6), will train Data Managers on best practices for organizing, editing, and transmitting data on the DCC web portal. CDC will develop a detailed manual describing study operations and procedures. The local NHBS Principal Investigator has responsibility for ensuring all HIV counselors are trained according to local guidelines and standards regarding HIV risk-reduction counseling and testing procedures.

4.1 Overview

As noted in Chapter 1, there are three main activities that make up venue-based sampling: 1) undertaking formative research to identify MSM venues, 2) sampling venues and day-time periods to create a monthly recruitment calendar, and 3) conducting recruitment events to enroll participants in the project. This chapter focuses on the latter two activities.

4.2 Monthly Recruitment Calendar

Each month, local project staff will create a recruitment calendar to schedule an upcoming month's recruitment events. The venues, days, and times (VDTs) for the recruitment events will be selected using a two-stage sampling method— the first stage to select venues and the second to select days and times.

4.2a Constructing sampling frames

Before sampling can begin, project staff will have to construct two sampling frames: a venue frame and a day-time frame. The venue frame is the list of venues *where* recruitment could potentially take place during the upcoming month, and the day-time frame is the list of day and time periods *when* recruitment could occur at each venue. Sampling frames should be continuously updated throughout the project period. As attendance patterns at venues change, day-time periods should be adjusted accordingly. Similarly, if new venues or day-time periods are identified, they should be added to the sampling frames. After both sampling frames have been constructed, sampling and VDT selection can begin.

4.2b Stage 1 sampling: venue selection

In stage 1 sampling, project staff select venues where recruitment will occur during the upcoming month. First, the staff determine the number of recruitment events they plan on conducting that month and then they randomly select a corresponding number of venues from the venue frame. In most cases, stage 1 sampling is done without replacement, meaning that once a venue has been chosen, it cannot be selected again that month, although it can be chosen as an alternate venue (see 4.2e below).

4.2c Stage 2 sampling: day-time period selection

In stage 2 sampling, project staff select the day-time periods when recruitment will occur at the venues chosen in stage 1. To facilitate the selection of day-time periods, project staff rank the venues chosen in stage 1 in order from the venue with the fewest number of day-time periods to

the venue with the most. Starting with the venue with the fewest number of day-time periods, project staff will randomly select a day-time period and schedule it on the recruitment calendar for the upcoming month. If no days are available on the recruitment calendar to schedule the event, another day-time period should be randomly selected from the remaining ones. Under the rare circumstance that the recruitment calendar cannot accommodate any of the day-time periods for a venue, a replacement venue is randomly selected from those that were not chosen in stage 1. The process of stage 2 sampling is repeated for each of the venues selected in stage 1 until all venues have been scheduled on the recruitment calendar. To minimize irreconcilable scheduling conflicts, venues should always be scheduled in order from the venue with the fewest number of day-time periods to the venue with the most. Although the day-time periods for conducting recruitment events are randomly selected in stage 2, the actual dates of the events on the recruitment calendar are not randomly selected in order to accommodate staffing needs.

4.2d Non-random recruitment events

Project staff may non-randomly select up to a maximum of three venues to include on their monthly recruitment calendar. These non-random events can be used to capture special events or to increase representation of important sub-populations, but they should be used sparingly. During the month that each project site holds its largest or main pride festival, they may conduct up to two additional non-random events at venues that are part of the main gay pride festival, for a total of five non-random events.

4.2e Alternate venues

Occasionally, recruitment cannot be conducted at a scheduled venue because of unforeseen circumstances like inclement weather or venue closure. Therefore, at least one alternate venue should be scheduled for each planned recruitment event. An alternate venue is randomly selected from among all the venues on the sampling frame that have a day-time period that corresponds to the day-time period of the scheduled recruitment event. The monthly recruitment calendar is complete when all sampled venues have been scheduled and alternate venues have been assigned for each one.

4.3 Recruitment Events

Each month, recruitment events are held at the venues scheduled on that month's recruitment calendar. During these events, project staff count venue attendees, recruit participants, screen for eligibility, conduct interviews, and test for HIV. Project sites will continue to hold recruitment events until they have enrolled a minimum of 500 MSM or until the NHBS-MSM3 end date.

4.3a Counting

A project staff member (usually the field supervisor) will count all men who appear to be ≥ 18 years of age who cross a defined area of the venue. This counting will last for the duration of the

recruitment event, beginning when the project staff are ready to start conducting interviews and ending when the last man has been approached for recruitment. Men are counted only once, even if they enter the defined area multiple times. Those men who have crossed the defined area of the venue and been counted form the pool of persons eligible for recruitment into NHBS-MSM3.

4.3b Recruiting

After a man has been counted, the staff member doing the counting will direct an interviewer or a designated recruiter to approach the man and attempt to recruit him for participation in the study. Men should be approached consecutively when project staff are available. Each recruiter will use an Intercept Form (Appendix D) during each recruitment event to record intercept data on the men who are approached. These intercept data are recorded on the forms in the presence of the potential participants. During recruitment, recruiters will briefly describe NHBS-MSM3, ask about previous participation in the survey, and for those who have not previously participated, ascertain willingness to participate. Men who have not previously participated in the survey, but are interested in doing so will be referred to an interviewer for eligibility screening. Men will normally be approached for recruitment in public, but eligibility screening occurs in a private area of the venue or in a designated interviewing space near the venue.

Appointments

In rare circumstances, if a potential participant does not wish to be interviewed at the time of recruitment, he can make an appointment to complete the survey at a later date. A future interview date and time could be scheduled before or after a recruitment event or the potential participant could call the project office to schedule one. In either case, the potential participant will be assigned a Survey ID. This anonymous number will be used to make the interview appointment, as well as to update recruitment monitoring forms. Interviews by appointment should be done sparingly and may only take place before or after a scheduled recruitment event or at the project office. The field supervisor, the interviewer, and at least one additional staff member must be in attendance during all interviews by appointment.

4.3c Eligibility screening and consent

Potential participants will be assessed for eligibility using the eligibility screener (Appendix E). If a potential participant is eligible, the interviewer will obtain informed consent from him by reading the consent form (Appendix F) and obtaining his verbal agreement to participate. Interviewers will address any questions that the participant may have prior to starting the survey.

If a potential participant is not eligible, he will be thanked for his time and interest in the project. No core survey data are collected on men who do not consent. However, they will be asked the reason why they are not interested in participating so that project staff can assess whether any barriers to the study exist.

4.3d Interviewing

Participants will be interviewed using the NHBS-MSM3 questionnaire (Appendix E) which is administered using a handheld, computer-assisted, personal interview program (HAPI). The interview will take about 30 to 40 minutes. Interviews are conducted in a private area of the venue or in a space near the venue.

4.3e HIV testing

Participants who consent to the survey, will be offered an anonymous HIV test. The testing component of NHBS-MSM3 is voluntary, and consent for HIV testing is obtained prior to survey participation. HIV counseling and testing must be conducted in accordance with the NHBS-MSM3 protocol (Chapter 5) and in accordance with local standards established by state and local health departments.

5.1 Overview

All persons who agree to participate in NHBS-MSM3 will be offered an anonymous HIV test. The testing component of NHBS-MSM3 is voluntary. The purpose of testing is to estimate HIV prevalence among men who have sex with men participating in NHBS. HIV counseling and testing must be conducted in accordance with the NHBS-MSM3 protocol and in accordance with standards established by state and local health departments.

Persons who agree to participate in the testing component of NHBS-MSM3 will be provided with information about HIV testing. In accordance with local procedures and practices, project sites may offer standard or rapid HIV testing to participants. A specimen will be collected and tested for the presence of HIV antigen or antibody from consenting participants. Serum or plasma specimens determined to be HIV-positive may be tested for evidence of recent HIV infection (incidence testing) if NHBS project sites choose to do so and local funds are used to support it. NHBS-MSM3 project sites that utilize the rapid HIV test will need to obtain additional specimens from participants with a preliminary positive (or reactive) result for confirmatory testing and, if applicable, incidence testing.

HIV test results will be returned to participants by a trained counselor during a scheduled counseling visit or shortly after the time of testing if a rapid test is used. Because results of incidence assays (see section 5.2e.2 below) are useful in the aggregate for estimating incidence as part of surveillance activities but are subject to considerable misclassification of individuals, Food and Drug Administration (FDA) regulations do not allow results of these assays to be returned to individuals or clinicians.

5.2 Procedures and Methods

5.2a Informed consent

Based on site-specific testing options, consent for NHBS-MSM3 will include: 1) participating in the survey; 2) testing blood or oral specimens for the presence of antigens and/or antibodies to HIV; 3) other tests (e.g., hepatitis, STD) provided locally; and 4) storing leftover sera for additional tests, including incidence testing and any other testing beyond local procedures for HIV diagnostic testing, when applicable. The informed consent process should follow local guidelines and standards with regard to HIV risk reduction counseling and testing procedures.

During the consent process, interviewers will explain to participants the purposes, procedures, benefits, and risks of giving a specimen and being tested for HIV. Participants may elect to

participate in the interview but refuse to provide consent for HIV testing. Participants who request an HIV test but do not consent to participating in NHBS-MSM3 will be given referrals and information for HIV testing. NHBS staff will also confirm a participant's decision to decline the HIV test at the end of the core survey to ensure they are given every opportunity to receive an HIV test. Appendix F contains a model consent form; if required, this form can be slightly modified to meet local requirements.

All tests done for NHBS-MSM3 will be anonymous. NHBS-MSM3 project sites unable to perform anonymous HIV testing will not be allowed to participate in NHBS-MSM3.

5.2b Local tests

NHBS project sites can conduct other tests in addition to an HIV test, provided local funds are used to support it. Tests that may be offered locally include sexually transmitted disease (STD) testing (e.g., syphilis) or hepatitis testing.

5.2c HIV counseling

After a participant consents to participating in NHBS-MSM3, survey administration is completed; next, HIV counseling and referrals are provided. Counseling for rapid and standard HIV testing should follow standards established by state and local health departments. Appropriate risk reduction counseling is provided to all participants who consent to HIV testing. Counselors will target prevention messages to specific risks identified during the behavioral surveillance interview. Barriers to risk reduction will be assessed, and methods to reduce or remove those barriers will be explored as appropriate for the participant. Counselors will provide referrals for any additional social support or medical services identified during the counseling session.

5.2d Specimen collection

NHBS project sites may choose the testing method most suitable for their local situation. Depending on laboratory needs, oral fluid specimens or blood specimens from fingerstick or venipuncture are collected for the purpose of HIV testing, although tests using blood tends to be more sensitive for early HIV infection than oral fluid. NHBS project sites may offer standard or rapid HIV testing to participants, although this choice may be impacted by the fact that test results will be anonymous and a proportion of persons will not return for test results. Those utilizing a rapid HIV test may collect specimens prior to survey administration, but only if local requirements allow counseling to be done after specimen collection, as counseling must not be done before the survey is administered. Project sites have the option to use a rapid testing algorithm as described in Appendix G. Persons who test preliminary positive for HIV on a rapid test must be asked to provide a blood or oral specimen for laboratory-based confirmatory testing at the time that preliminary positive test results are given. Results for rapid tests and specimen collection for confirmatory testing should be available after the survey has been administered. For NHBS project sites that choose to do incidence testing, incidence tests will be conducted on

remnant samples of the confirmatory specimen. Processing of specimens should be done according to appropriate laboratory methods for the type of specimen collected.

Specimens are labeled with unique Survey ID numbers that match the participant's lab slip, questionnaire, and counseling card. No patient identifiers are included on any survey, specimen, lab slip, or instrument; this includes any tests provided locally (e.g., STD testing). The unique Survey ID is also affixed to the participant's appointment card, and the participant is counseled to keep the card in order to receive his/her results.

The NHBS Project Coordinator and collaborating technician at the laboratory will maintain a log of all samples received for NHBS. This log will contain the participant's Survey ID, the time and date of specimen collection and information regarding the participant's consent for storage. If the participant consents to storage, the log will indicate the date and time the sample was processed for storage and the amount frozen. If the participant does not consent to storage, the log will indicate the date and time the sample was destroyed. NHBS Project Coordinators will work closely with the lab to ensure the proper storage and disposal of NHBS specimens.

5.2e Counseling/returning HIV test results

Participants who are provided with rapid HIV testing will receive their results during the NHBS-MSM3 encounter. Reactive (preliminary positive) test results obtained through the currently approved HIV rapid tests require that a confirmatory test (e.g., Western Blot, IFA, p24 antigen, nucleic acid detection) be conducted in a laboratory (CDC, 1989; CDC, 1998; CDC, 2004). Confirmatory tests acceptable for NHBS are those which are consistent with the current HIV case definition (CDC, 2008).

Those participants who do not undergo rapid testing will receive their final HIV test results by trained counselors within one to three weeks of the date of the specimen collection. NHBS-MSM3 project sites should develop flexible systems for return of HIV test results and counseling that are easily accessible by participants. During the initial encounter, the counselor will work with the participant to schedule a post-test counseling session. The participants should be given an appointment card with the name and telephone number of health department personnel or counselor and the date, time and location of their appointment. The appointment card must have an affixed Survey ID number to link test results to the patient. No personal identifying information will be linked to the participant's HIV test result.

In the event that an in-person counseling session cannot be scheduled, participants may elect to receive HIV test results by telephone but only if local requirements allow the return of results in this manner. Appendix H includes an example of a detailed Telephone HIV Test Result Protocol used in Los Angeles as Part of *Project 1* (Protocol # 3910). NHBS project sites providing HIV results over the telephone must provide appropriate training to all telephone counselors.

All participants who test positive for HIV antibodies or antigens should be referred for appropriate medical care and HIV case management services at the time they receive their

confirmatory test results. NHBS project areas performing rapid testing may elect to make a referral to care for participants with preliminary positive results at the time of the NHBS encounter during post-test counseling and after a confirmatory specimen has been collected. All referrals must be anonymous and the participant may not be reported to the state or local health department for HIV/AIDS surveillance purposes. The HIV test result can only be used for NHBS analysis purposes.

5.2f Incidence Testing and Results

Advances in laboratory technology allow for the antibody testing of HIV-positive blood specimens from cross-sectional surveys to classify them as recent versus longstanding infection for the purpose of calculating HIV incidence estimates. There are several candidate incidence assays, but none have won wide acceptance. To date, the only incidence assay that has been FDA-approved is the BED HIV-1 Capture EIA assay (Parekh et al., 2001). The FDA has determined that the BED assay, when used for surveillance purposes, does not require an Investigational New Drug or Investigational Device Exemption (Appendix I). Because the safety and effectiveness of this assay have not been established for purposes other than estimating HIV incidence at a population level, ***FDA regulations prohibit providing results to individuals*** or using these results for clinical management.

Incidence assays can only be performed on blood specimens (e.g., serum, plasma, etc.) determined to be HIV positive. Therefore, sites interested in measuring HIV incidence must collect blood specimens from participants. Project sites should first consult with the laboratory performing the incidence testing to determine the type of specimens accepted for incidence assays. Incidence testing for NHBS-MSM3 is optional for project sites and can only be done provided local funds are used to support it and participants consent to specimen storage. Plans for incidence testing must be discussed with a CDC Project Officer.

As with the BED assay, any incidence assay performed on NHBS specimens can only be used to estimate the incidence in that population. The results are for public health purposes only and cannot be used on an individual basis, i.e., returned to an individual.

5.2g Reimbursement

HIV antibody tests will be provided at no cost to participants. In addition, participants may be reimbursed approximately \$25 for their time after all biologic specimens have been collected.

If local policy allows participants to receive reimbursement for returning for their HIV test results, project sites may do so, provided NHBS funds are not used for that purpose. Project sites considering reimbursing participants for returning for their HIV test results must discuss this with their CDC Project Officer before implementation.

5.2h Data collection

The NHBS lab coordinator will maintain a log of all specimens received. The log will contain:

- unique Survey ID;
- time and date of specimen collection;
- time and date the specimen was processed;

If consent for storage is obtained:

- time and date the sample was frozen;
- amount of sample frozen; and
- date and amount of frozen sample sent to CDC or a designated laboratory.

The log should be secured in a locked file cabinet. Access to the log should be limited to designated project staff.

Results of the HIV test will be recorded on a data collection form completed by the laboratory personnel or by the NHBS-MSM3 project staff from a copy of the HIV test results. Results of testing (including those for recent infection) will be linked to interview data via the unique survey ID. All laboratory results (lab slips or print outs) will be stored in a secure and locked cabinet.

5.3 Data Management

HIV test results will be entered into the HIV Test Result Log on the Data Coordinating Center (DCC; see chapter 6) Data Portal's online database. These data will be entered at least weekly so that reports generated by the DCC will reflect project sites' current numbers. A model HIV testing log is found in Appendix J.

6.1 Overview

The purpose of this chapter is to describe basic data management procedures. The format for specific databases and directions for submitting data will be developed in collaboration with CDC and participating sites.

6.2 Data Configuration

6.2a Data Files

Each NHBS-MSM3 project site will maintain the following 5 databases:

1. QDS Warehouse for the NHBS-MSM3 questionnaire
2. QDS Warehouse for local questions
3. Recruitment Monitoring Database
4. HIV Testing Database
5. Venue Day Time Sampling (VDTS) Database

To ensure consistency in database layouts across the NHBS-MSM3 project sites, CDC will develop a QDS (Questionnaire Development System) control file with specifications for the interview data. QDS is software used to program survey development, collect data, and manage data collection. These specifications will cover the questions, variable names, field limits, consistency checks, response values, and formats. The control file will be programmed such that cycle specific (MSM, IDU or HET) questions are asked during the appropriate cycle. CDC will also ensure consistency in database layouts for the Recruitment Monitoring database, Venue Day Time Sampling (VDTS) database and the HIV testing database. Specifications will cover variable names, field limits, response values, and formats.

6.2b Data Submissions to CDC

All data submissions to the CDC are made to the Data Coordinating Center (DCC). The DCC collects and processes data for delivery to the CDC as well as sites. Data management procedures performed by the DCC use standard data processing tools such as SQL and SAS. These include managing incoming data, generating error reports, incorporating data changes, and producing CDC required management reports. Data is transmitted to the DCC either by file upload (e.g., QDS Warehouse) or direct data entry (e.g., Data Error Log, HIV testing data, etc.) using secure data entry screens within the web-based data portal system. In addition to sending data to DCC, the portal can also be used by sites to revise submitted data, view reports, track field site activities and retrieve processed datasets.

After the NHBS-MSM3 data are sent through the DCC web portal, they will be processed by the DCC data manager. The DCC will then produce a report, on a monthly basis, for each NHBS-MSM3 project site that lists any data inconsistencies; the project sites will respond to the DCC's report, and the edits will be incorporated into the data sets.

During the course of NHBS-MSM3, project sites should communicate problems to both their Project Officer and to DCC representatives in order to resolve these issues in a timely manner.

Representatives from the DCC will train Data Managers on best practices for organizing, entering, editing and transmitting data on the DCC web portal. Data Managers will also receive a detailed manual that will list all requirements for maintaining NHBS data sets; this manual shall be the primary resource for conducting NHBS-MSM3 data management activities.

6.3 NHBS-MSM3 Analysis File

After the conclusion of the NHBS-MSM3 cycle, the DCC will create a standardized dataset (or a program to create the dataset locally) for each project site. NHBS-MSM3 project sites will only receive their site-specific dataset. The purpose of the standardized datasets is to ensure that reports of NHBS-MSM3 data are consistent at both the local and national level.

7.1 Data Analysis and Dissemination

CDC will have principal responsibility for analyzing and disseminating multi-site survey and HIV testing data. The CDC analyses will focus primarily on questions related to the objectives of this study, as described in Chapter 1. To examine these key behavioral surveillance outcomes, data may be weighted to account for the complex sampling design, which includes venue and day-time period sampling, as well as counts of venue attendees.

NHBS project sites have responsibility for analyzing and disseminating site-specific data. Project sites are encouraged to establish Community Advisory Boards (CABs) or other organizations to transmit study findings to the target community and its stakeholders.

7.1a Outcomes and minimum meaningful differences

Anticipated outcomes for this study are:

- Prevalence of unprotected anal sex in the past 12 months;
- Prevalence of multiple male sex partners in the past 12 months;
- Prevalence of injection and non-injection drug use in the past 12 months;
- Prevalence of HIV testing and, among those tested, percentage who got their results;
- Prevalence of HIV infection, including previously undiagnosed HIV infection;
- Prevalence of receiving HIV prevention services in the past 12 months.

Minimum meaningful differences will vary depending on the outcome of interest, but are expected to be between 5% and 20%.

7.1b Anticipated products

NHBS-MSM3 will result in national and local products and publications. CDC is responsible for disseminating national reports, usually via the *Morbidity and Mortality Weekly Report* (MMWR) and peer-reviewed journals. CDC will also present findings at national conferences and meetings. Local NHBS project sites are responsible for disseminating local NHBS-MSM3 results to health department officials and the public by presenting findings at conferences, preparing reports for community planning groups, or publishing results in peer-reviewed journals. NHBS project sites and CDC may collaborate on articles and reports when appropriate.

7.2 Limitations and Potential Biases

7.2a Venue-based sampling

Findings from venue-based sampling methods can only be generalized to the population of eligible persons attending venues included on the sampling frame during the surveillance cycle (MacKellar *et al.*, 1996; CDC, 2006; MacKellar *et al.*, 2007). Some persons who are otherwise eligible (*e.g.*, by age, sexual behavior, and residence) may not attend the venues on the sampling frame or not attend venues at all. To minimize the effect of this bias, formative research is conducted throughout the data collection period to update venue and day-time period sampling frames.

Despite these limitations, venue-based sampling has obtained large and diverse samples in other studies, including NHBS-MSM1 and NHBS-MSM2.

7.2b HIV testing

Biases in enrollment and consent to HIV testing may result in over- or under-estimation of HIV prevalence. If those who agree to be tested differ from those who decline in terms of demographic characteristics or risk behaviors, our findings may be less generalizable.

8.1 HIV/AIDS Surveillance Assurance of Confidentiality

As a component of HIV/AIDS surveillance, NHBS data are protected by the Assurance of Confidentiality (Section 308(d) of the Public Health Service Act, 42 U.S.C. 242 m(d)). This assurance prohibits the disclosure of any information that could be used to directly or indirectly identify individuals. A copy of the *Assurance of Confidentiality for HIV/AIDS Surveillance Data* is provided in Appendix K.

8.2 Written Data Security Policy

In accordance with the Assurance of Confidentiality requirements, each funded health department will write a data security policy covering the NHBS data and incorporate it into their existing policy for HIV/AIDS surveillance data. The written data security policy should be approved by the Overall Responsible Party (ORP) at the funded health department prior to implementing data collection. Until this is done, NHBS project sites must apply their existing standards for HIV/AIDS surveillance, which are approved by the ORP, to the NHBS data. For guidance on developing data security policies for HIV surveillance data, consult the CDC *Guidelines for HIV/AIDS Surveillance* (see Appendix L), which establishes minimum data security standards for protecting HIV/AIDS surveillance data.

The written policy will describe:

- The standard operating procedures and policies for maintaining the security of NHBS data.
- A data release policy describing the provisions for protecting against access to raw data or data tables containing small-denominator populations that could be indirectly identifying.
- An evaluation of the data security measures outlined in the document.

8.3 Security and Confidentiality Requirements

The following are the most applicable requirements for protecting the security of NHBS data. They are not inclusive of all the requirements listed in the *Guidelines for HIV/AIDS Surveillance* (Appendix L). Therefore, while drafting the local data security policy, NHBS project staff should not rely solely on the requirements provided in this document.

8.3a Maintain anonymity of the participants

- Participant names should not be included in any NHBS data collection instruments or systems, including QDS programs, VDT sampling information, recruitment monitoring forms and lab slips or test results. The only number used to label and identify data from the same participant is the Survey ID. If written consent forms are used and local policy requires participants to sign their real names to the forms, the consent forms should not be labeled with the Survey ID and are to be maintained in a separate file from other NHBS instruments. NOTE: Consent for all NHBS participants will be documented using the handheld computer and will be a part of each participant's survey record.
- If an appointment system is used for interviews, the appointment form will identify a prospective participant by the Survey ID.
- In the event that a local policy requires participants to indicate they received an incentive, it is recommended that the Survey ID be used to identify the participant and NOT the participant's name or signature. If policy will not allow the use of the Survey ID in lieu of the name or signature, special care should be taken to ensure that the Survey ID is not included on the form and that the form is stored separately from NHBS instruments. In either case, any receipts should not describe the project or contain the name of the NHBS project.
- Specimens, lab slips, and questionnaires are to be linked using the Survey ID number and the interview date. No personal identifiers should be written or affixed to the test results or lab slips. All HIV tests, including confirmatory tests, must be conducted anonymously. Any additional tests offered locally must also be anonymous.

8.3b Protect the electronic security of surveillance databases

- Computers that can access electronic NHBS data should be physically secured and should be protected by coded passwords.
- Electronic databases containing NHBS data should be protected using coded passwords.
- Only authorized persons are to have access to electronic NHBS databases. Only individuals within the health department (and the authorized contractors) should be authorized to access NHBS data. Access to NHBS data must be defined in a formal, written data release policy.
- Access to data by personnel outside the surveillance unit must (1) be limited to those authorized on the basis of an expressed and justifiable public health need, (2) not compromise or impede surveillance activities, (3) not affect the acceptability of the surveillance system, and (4) be approved by the State ORP.

- Handheld computers
 - Handheld computers must be kept in the possession of the field staff at all times when in the field. Although the data management module of QDS is the only module that allows viewing of completed and entered interviews in the QDS files, the HAPI module of QDS (used to launch the NHBS questionnaire on the handheld computers) can view incomplete interviews. Handheld computers incorporate the use of encryption software. NHBS data must be encrypted when stored on a handheld device. The key for de-encryption must not be written on the handheld device. Since NHBS interviews are encrypted by QDS and the de-encryption key is in the QDS warehouse module, the QDS warehouse should not be loaded on handheld device. Handheld computers must be protected by using a coded password known only to authorized NHBS project staff. Handheld computers must be collected and secured by the field supervisor after the last interview of the day. When not in use in the field, the handheld computers are to be locked in a drawer or office at the health department or the contracted agency conducting the surveillance. If this is not feasible, then a plan should be developed and incorporated into the data security policy that will ensure the security of the handheld computers.
 - Handheld computers must be purged of NHBS data after the last interview of the day by uploading the collected interviews to the main database (e.g. QDS warehouse). This is important to minimize the amount of data carried on the handheld device. It will also minimize the number of records lost or compromised if the handheld device is lost or stolen.
- The ORP, NHBS Principal Investigator, and the CDC project officer must be notified in the event that a computer (including handheld computers) containing NHBS data is lost or stolen.
- When a computer used for NHBS is taken out of service, any hard drives that may have once contained NHBS data should be reformatted before being used for another purpose.
- Other removable storage media (e.g., compact disks used to store data backups) that are no longer needed for NHBS should be destroyed and not used for another purpose.

8.3c Protect the transmission of electronic data

NHBS data will be transmitted to DCC using the DCC portal, a secure internet based file transfer system hosted by the DCC. Data submitted thru the DCC portal should be encrypted before being uploaded.

Surveillance data may not be transmitted through email or on disk because copies of the data will be maintained on various servers. A secure method for transmitting data files between local computer systems must be identified. Transfer files containing the NHBS data must be encrypted using commercially available software with at least 128-bit encryption capability.

Encrypted databases may be transferred to a diskette or compact disk (CD) that can then be delivered by a courier service with package tracking capability (e.g., Federal Express or UPS) to an authorized individual who can upload the data to the other computer system.

The use of modems for data transfers must be approved by the ORP and incorporate the use of access controls. In addition, the NHBS data must be encrypted prior to electronic transfer.

8.3d Protect the physical security of paper copies of NHBS forms

- Paper copies of consent forms and other NHBS forms must be stored in locked filing cabinets that are inside locked offices.
- Only authorized persons should have access to paper copies of NHBS forms.
- Paper copies of completed consent forms and NHBS forms should be kept secured while interviews are being conducted in the field. Interviewers should use a clipboard or other device to gather these files during office hours and maintain possession of them throughout the field event. Field supervisors must gather all paper copies of completed consent forms and NHBS forms at the end of each field event and store them in a locked cabinet at the health department or within the field office.

8.3e Require project staff to take individual responsibility in protecting data

- All authorized NHBS project staff must sign a confidentiality statement (see example in the attachments to the CDC *Guidelines for HIV/AIDS Surveillance*, Appendix L). Newly hired staff must sign a confidentiality statement before access to NHBS data is authorized. This statement must indicate that NHBS data will not be released to unauthorized individuals. The original statement must be held in the employee's personnel file and a copy given to the employee. Staff must sign the confidentiality statement on an established periodic basis (e.g., annually).
- All authorized NHBS project staff with access to data must be knowledgeable about the data security policies and procedures. The written data security policy should be readily available and data security awareness trainings should be provided at regular intervals.
- NHBS project staff should not discuss the participants or the information shared during the questionnaire interviews with any unauthorized individual. Interviewers may share information with field supervisors or other study managers who have authorized access to NHBS data for problem-solving issues that arise in the field.
- Each NHBS project staff member will be responsible for protecting his/her workstation, laptop or handheld device that contains NHBS data. This responsibility includes protecting the keys to the physical space (e.g., offices), passwords, and other codes that would allow access to sensitive data. In addition, NHBS project staff must take care not to infect the computers with viruses or damage the equipment through exposure to the elements or misuse.

- NHBS project staff must not install software on the handheld computers or laptops containing NHBS data without notifying the CDC project officer.
- NHBS project staff should keep completed NHBS forms secured while interviewing in the field; use of clipboards or other devices that are in the possession of the interviewer at all times during field operations is recommended for this purpose.
- NHBS project staff must shred documents containing sensitive information before disposing of them.

8.4 Breaches in Data Security Procedures

Breaches in the data security procedures should be promptly investigated by NHBS-MSM3 staff to assess the causes and implement remedies. Confirmed breaches resulting in the release of sensitive information should be reported to the ORP, the NHBS Principal Investigator, and the CDC Project Officer within two (2) business days of the adverse event.

9.1 Institutional Review Board Approval

The protocol for NHBS Round 2, was submitted for review and approved by CDC's Institutional Review Board (IRB) in 2007. In April 2009, the CDC Human Research Protections Office subsequently determined that NHBS is research, but that CDC is "not engaged" in this research. Therefore, the NHBS-HET2 protocol was not reviewed by the CDC IRB. In November 2010, the CDC Human Research Protections Office determined that NHBS Round 3 is research, but that CDC is "not engaged" in this research. Because NHBS is considered research, NHBS-MSM3 project sites must submit this protocol to their state and local IRBs for full or expedited IRB review; the state or local IRB of record may not determine the NHBS-MSM3 amended protocol to be exempt from review.

Participation in formative research activities involves the completion of an anonymous interviewer-administered interview or facilitator-led focus group. Consent will be obtained for interviewer-administered key informant interviews (Appendices A and B) and facilitator-led focus groups (Appendix C). Participation in the surveillance activities involves the completion of an anonymous interviewer-administered risk behavior survey and voluntary HIV counseling and testing (Appendix M). The interviewer will document consent in the handheld computers used for interviewing by indicating whether consent was obtained for the survey, for HIV testing and, where applicable, other tests (e.g., hepatitis) or specimen storage.

9.1a Justification of waiver of documentation of informed consent

For this protocol, a waiver of documentation of informed consent is recommended. The only record linking the subject and the research would be the consent document, and the principal risk would be the potential harm resulting from a breach of confidentiality. This protocol presents no more than minimal risk of harm to subjects. NHBS-MSM3 Principal Investigators should request a waiver of documentation of informed consent to allow the use of oral consent (Appendix M) on the basis that the research presents no more than minimal risk of harm to subjects and involves no procedures for which written consent is normally required outside of the research context.

9.2 Potential Risks and Anticipated Benefits

Participation in NHBS-MSM3 presents no more risks to respondents than that which might occur outside of the context of surveillance. These non-surveillance contexts include participation in individual or group HIV prevention activities and interactions with HIV prevention and health-care providers in public or clinical settings. Similar to these contexts, participating in NHBS-MSM3 might cause discomfort to those participants who do not recognize their risks for

HIV/STD infection. Although privacy will be protected to the greatest extent possible, some acquaintances may recognize those respondents who are approached in public settings and who choose to participate.

9.2a Risks and benefits of the survey

Participants may benefit from participating in the NHBS-MSM3 survey by better recognizing their own risks for HIV infection, speaking to trained staff about how to reduce those risks, learning more about local HIV prevention efforts, and obtaining prevention materials and referrals for health care, drug treatment, or HIV/STD testing and prevention services. Participating in NHBS-MSM3 also benefits communities by helping prevention planners to better direct state and local HIV prevention efforts.

Participants may feel uncomfortable about some of the questions in the survey, particularly those that are about sex and drug use.

9.2b Risks and benefits of HIV testing

The risks of participating in the HIV testing component of NHBS-MSM3 are minimal and include those associated with loss of anonymity, drawing blood, and returning test results. Drawing blood may cause temporary discomfort such as bruising and rarely, infection. Some persons may pass out, and some have become injured while having their blood drawn; both of these circumstances are rare. There is minimal risk of secondary infection associated with phlebotomy. Disclosure of a confirmed reactive HIV test result may cause substantial psychological trauma. A preliminary positive result from a rapid HIV test may cause temporary distress until the confirmatory results are available.

Individuals who agree to participate in HIV testing will receive counseling about how to prevent acquiring or transmitting HIV infection and, if appropriate, referral to local programs, support groups and health care providers.

9.3 Voluntary Participation

Participation in NHBS-MSM3 is completely voluntary. Participants can refuse to participate in the NHBS-MSM3 survey or in the HIV testing component without penalty. Participants are not required to take an HIV test to participate in the survey. However, participants will not be able to receive an HIV test without first completing the NHBS-MSM3 survey. Once participants have started the survey, they can refuse to answer any question or end the survey at any time without penalty. Participants who NHBS project staff deems mentally incompetent to give informed consent, including those who are inebriated with alcohol or drugs, will not be allowed to participate in the interview.

All consent forms, questionnaires, and other survey instruments will be professionally translated into Spanish and certified. All consent forms, questionnaires, and survey instruments in Spanish will be administered by Spanish-speaking NHBS-MSM3 project staff.

9.4 Vulnerable Populations

Persons under the age of 18 years of age will not be included in NHBS-MSM3. Prisoners will not be included in NHBS-MSM3. Women will not be included in NHBS-MSM3; no special procedures are required for the participation of pregnant women. Persons with mental disabilities may also be included; however any person who cannot provide informed consent will be excluded from participation in the project. Interviewers will be trained to identify participants who cannot provide informed consent; these persons will be given the opportunity to reschedule their appointment as appropriate. All participants will be afforded the same protections.

9.5 Informed Consent Process

Participants will take part in an informed consent process prior to beginning the survey. A model statement of informed consent is provided in Appendix F. Because participants may have difficulty reading and comprehending a written consent form, consent information should be read to each participant.

Documentation of obtaining consent will be entered into the HAPI program after the eligibility screener is administered. The HAPI program will automatically end the NHBS-MSM3 survey questionnaire if the respondent does not agree to participate. Respondents have the option of participating in the survey but declining the HIV test or other tests that are being offered. Sometimes, participants may change their mind about taking the HIV test during survey implementation; therefore, participants who initially decline the HIV test will be offered another opportunity at the end of the survey to receive the HIV test as part of the study. NHBS respondents are not required to agree to receive the results of their HIV test in order to participate in the study.

Participants will be offered a copy of the consent forms to read along with the interviewer; they may keep the form if they wish. Consent scripts or forms developed by NHBS-MSM3 project sites must contain all required elements of informed consent (Appendix N). Each NHBS-MSM3 project site's consent script or form must be reviewed and approved by the respective CDC project officer before submission to the local IRB.

9.6 Age of Participants

Investigators at CDC and eligible grantee institutions have experience recruiting participants in the proposed age range and the proposed types of venues (Valleroy, 2000; Muhib, 2001; Stueve,

2001; MacKellar, 2007). NHBS is a surveillance system of the HIV risk behaviors of adults in the United States, and the methods used in NHBS-MSM3 are designed to recruit an adult population. Previous studies have used the same age criteria as proposed for NHBS-MSM3 and successfully recruited participants aged 18 and older (CDC, 2006). The venue facilities where recruitment and interviewing will occur generally attract a wide range of participants; a broad mix of venues ensures that younger participants who may not be old enough to enter bars and clubs still have a chance to participate.

Persons younger than 18 years of age are excluded from this research because a separate, age-specific study of persons less than 18 years old is warranted and preferable. Sufficient numbers of subjects less than 18 years of age would be needed for age-specific analyses to be meaningful.

9.7 Anonymity and Privacy Protections

NHBS-MSM3 is covered under the *Assurance of Confidentiality for HIV/AIDS Data* (Appendix K).

9.7a Anonymity protections

Participation in NHBS-MSM3 is anonymous. Participants will not be required to provide their names or other personal identifiers as a condition for participation. In order to prevent inadvertent linkage, consent forms that must be signed (due to local IRB requirement) are not labeled with a Survey ID number and are maintained separately from other documents. Blood specimens, lab slips, and questionnaires are linked by Survey ID numbers only. No personal identifiers are on any of these forms. If participants voluntarily disclose their names or personal identifiers, these will not be maintained by NHBS-MSM3 project staff nor linked with any survey instrument.

In some cases, prospective participants recruited during the recruitment event have the opportunity to make appointments to complete the NHBS-MSM3 survey at a later date. These prospective participants will be assigned an anonymous survey number for appointment scheduling. Participants who must return for HIV test results should be given post-test interview cards labeled only with Survey ID numbers that link respondents with test results.

9.7b Privacy protections

NHBS-MSM3 project staff will always conduct surveillance activities in ways that adhere to the ethical principles and standards by respecting and protecting to the maximum extent possible the privacy, confidentiality, and autonomy of participants.

Paper copies of NHBS-MSM3 consent forms, test results or other forms will be stored in locked filing cabinets that are maintained in secure office environments with limited and controlled access. Equipment used to administer the CDC-developed HAPI program (including handheld

computers) will be password protected. Computers and networks where data will be downloaded and stored will also be password protected. Only authorized project staff will have access to completed survey data and study files. All project staff that will have access to the NHBS-MSM3 data must undergo local security and confidentiality training and must sign a statement of confidentiality.

The NHBS-MSM3 project sites will send data to CDC using the Data Coordinating Center (DCC), managed by ICF Macro. The DCC must use the secure data transfer algorithm, FIPS 140-2 (Federal Information Processing Standards Publication). Information about the algorithm can be found at this web-site (<http://www.csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>). The secure data transfer methodology is compliant and meets the guidelines set forth in OMB memorandum M-0404 (E-Authentication Guidance for Federal Agencies) (<http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>) and NIST Special Publication 800-63 (E-Authentication Guideline: Recommendation of the National Institute of Standards and Technology) (http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf). The DCC data management systems must be in compliance with OMB, HHS, and CDC Certification and Accreditation Guidelines outlined in NIST SP 800-37 (Guide for the Security Certification and Accreditation of Federal Information Systems) (<http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf>). In addition to the technical requirements listed above, data management processes must be in compliance with The Guidelines for HIV/AIDS Surveillance – Security and Confidentiality. (<http://www.cdc.gov/hiv/topics/surveillance/resources/guidelines/guidance>)

9.8 Reimbursement for Time and Effort

Activities that are part of NHBS-MSM3 include the survey (which is the only activity required for participation) and taking a voluntary HIV test. Participants will receive a small stipend for participation in NHBS-MSM3 activities. The reimbursement amounts are determined locally by the NHBS-MSM3 project sites; amounts included in this document are based on previous experience with NHBS cycles or other similar studies.

Respondents will be reimbursed approximately \$25 in cash for their participation in the NHBS-MSM3 survey. If local regulations prohibit cash disbursement, equivalent reimbursement may be offered in the form of gift certificates; however, all non-cash reimbursements should have appropriate value to the population. The formative research process can help verify what types of non-cash reimbursements are appropriate. All participants will be offered referrals to and materials with appropriate prevention information, testing resources, medical services, and other support services.

HIV antibody tests will be provided at no cost to participants. In addition, participants will be reimbursed approximately \$25 for their time and inconvenience. Appropriate risk-reduction counseling will be provided to all participants who elect testing for HIV. Interviewers will target prevention messages to specific risks identified from the survey questionnaire. Barriers to risk

reduction will be assessed, and methods to reduce or remove those barriers will be explored as appropriate for the participant.

Participants will receive their stipend after the survey has been administered and the specimen collected for HIV testing (if participant agrees to the HIV test). Project sites may choose to have either the Field Supervisor or the Interviewer dispense the stipend.

9.9 Adverse Events

9.9a Definition of an adverse event

In NHBS-MSM3, adverse events are defined as events leading to serious psychological, social, or physical harm to a participant that result from his or her participation in the study, including responding to the survey, and that are reported to or observed by any project staff. Adverse events should be distinguished from the mild, transient, and normal discomfort or awkwardness that some participants may experience during risk behavior interviewing (such as fidgeting in the seat, seeming apprehensive when speaking, not looking at the interviewer or looking down, blushing).

9.9b Examples of adverse events

- **Violations of confidentiality or privacy.** Having information about their participation disclosed by a member of NHBS-MSM3 project staff.
- **Hazing, harassment, or violence.** Examples are emotional trauma, physical violence or verbal abuse directed at a participant or project staff as a result of taking part in an interview.
- **Negative reactions from the community.** An example is a participant losing housing or other services because of participation in the study.
- Complaints about inappropriate **behavior on the part of NHBS-MSM3 project staff.**
- **Psychological or physical trauma** as a result of HIV testing.
- **Violations of the NHBS-MSM3 protocol.**

9.9c Response to adverse events

Adverse events must be taken seriously and handled in a consistent manner by all NHBS-MSM3 project staff. The field supervisor must be notified of the event within 24 hours. The field supervisor will determine whether the reported event was related to NHBS-MSM3 and will document and report the event and its outcome. Adverse events determined to be related to NHBS-MSM3 must be reported to CDC and the local IRB within 2 business days or earlier as

mandated by local IRB guidelines; the CDC NHBS staff will report adverse events to the Associate Director for Science in the Division of HIV/AIDS Prevention for review and follow-up.

NHBS project staff are trained to respond to emergency situations involving NHBS-MSM3 participants, such as if a participant expresses suicidal feelings upon receiving a positive HIV test result. NHBS personnel are locally trained to respond to questions and concerns from participants who consent to HIV testing. They are also trained in de-escalation techniques, and how to respond to emergencies (e.g., fire/police/hospital contact numbers).

References are listed in alphabetical order. The chapter in which the reference is cited is listed in parentheses at the end of the citation.

Centers for Disease Control and Prevention. Interpretation and use of the Western blot assay for serodiagnosis of human immunodeficiency virus type 1 infection. *MMWR*. 1989; 83 (No. S-7). (*Chapter 5*)

Centers for Disease Control and Prevention. Update: HIV Counseling and Testing Using Rapid Tests—United States, 1995. *MMWR*. 1998; 47 (11): 211-215. (*Chapter 5*)

Centers for Disease Control and Prevention. Notice to Readers: Protocols for Confirmation of Reactive Rapid HIV Tests. *MMWR*. 2004; 53 (10): 221-222. (*Chapter 5*)

Centers for Disease Control and Prevention. Revised Surveillance Case Definition for HIV Infection. *MMWR*. 2008; 57 (No. RR-10). (*Chapter 5*)

Centers for Disease Control and Prevention. CDC HIV prevention strategic plan through 2005. Available at: www.cdc.gov/nchstp/od/hiv_plan/default.htm, 2001. (*Chapter 1*)

Centers for Disease Control and Prevention. HIV prevalence, unrecognized infection, and HIV testing among men who have sex with men -- five US cities, June 2004-April 2005. *MMWR* 2005;54:597-601. (*Chapter 1*)

Centers for Disease Control and Prevention. Surveillance summary: human immunodeficiency virus (HIV) risk, prevention, and testing behaviors -- United States, National HIV Behavioral Surveillance System: men who have sex with men, November 2003-April 2005. *MMWR* 2006;55(SS06):1-16 (*CDC, 2006; Chapters 1, 7, and 9*)

Centers for Disease Control and Prevention. Trends in HIV/AIDS diagnoses among men who have sex with men -- 33 states, 2001-2006. *MMWR* 2008;57(25):681-686. (*CDC, 2008a; Chapter 1*)

Centers for Disease Control and Prevention. HIV prevalence estimates -- United States, 2006. *MMWR* 2008;57(39):1073-1076. (*CDC, 2008b; Chapter 1*)

Centers for Disease Control and Prevention. Youth risk behavior surveillance -- United States, 2007. *Surveillance Summaries*, 2008. *MMWR* 2008;57(No. SS-4). (*CDC, 2008c; Chapter 1*)

Centers for Disease Control and Prevention. Prevalence and awareness of HIV infection among men who have sex with men -- 21 cities, United States, 2008. *MMWR* 2010;59(37):1201-1207. (*Chapter 1*)

Diaz RM, Ayala G, Bein E, Henne J, Marin BV. The impact of homophobia, poverty, and racism on the mental health of gay and bisexual Latino men: Findings from 3 US cities. *American Journal of Public Health* 2001; 91(6):927-932. (*Chapter 1*)

Gallagher K, Sullivan, P, Lansky, A, et al. Behavioral surveillance among people at risk for HIV infection in the U.S.: The National HIV Behavioral Surveillance System. *Public Health Reports* 2007; 122(suppl 1):32-38. (*Chapter 1*)

Hall HI, Song R, Rhodes P, et al. Estimation of HIV incidence in the United States. *JAMA* 2008;300:520-529. (*Chapter 1*)

Higgins DL, O'Reilly KR, Tashima N, et al. Using formative research to lay a foundation for HIV prevention: An example from the AIDS Community Demonstration Projects. *Public Health Reports*. 1996; III (supplement):28-35. (*Chapter 2*)

Kreuger RA and Casey MA. *Focus Groups: A practical guide for applied research*. Thousand Oaks, CA: Sage Publications. 2000. (*Chapter 2*)

Lambert EY, Ashery RS, and Needle RH, editors. *Qualitative methods in drug abuse and HIV research*. National Institute on Drug Abuse Research Monograph Series, No. 157. U.S. Department of Health and Human Services, 1995. (*Chapter 2*)

Lansky, A, Sullivan, P, Gallagher, K, et al. HIV behavioral surveillance in the U.S.: a conceptual framework. *Public Health Reports* 2007; 122(suppl 1):16-23. (*Chapter 1*)

MacKellar D, Valleroy L, Karon J, et al. The young men's survey: methods for estimating HIV seroprevalence and risk factors among men who have sex with men. *Public Health Reports* 1996; 111(suppl 1):138-144. (*Chapters 1 and 7*)

MacKellar DA, Valleroy LA, Secura GM, et al. Unrecognized HIV infection, risk behaviors, and perceptions of risk among young men who have sex with men: opportunities for advancing HIV prevention in the third decade of HIV/AIDS. *Journal Acquired Immune Deficiency Syndrome*. 2005;38:603–14. (*Chapter 1*)

MacKellar D, Gallagher K, Finlayson T, et al. Surveillance of HIV risk and prevention behaviors of men who have sex with men – a national application of venue-based, time-space sampling. *Public Health Reports* 2007; 122(suppl 1):39-47. (*Chapters 1, 7, and 9*)

Muhib F, Lin L, Stueve A, et al. A venue-based method for sampling hard-to-reach populations. *Public Health Report*. 2001;116(suppl 1):216-222. (*Chapters 1 and 9*)

Needle RH, Trotter II RT, Bates C, Singer M . Rapid Assessment, Response, and Evaluation (RARE) Project Training Workbook. U.S. Department of Health and Human Services: Office of HIV/AIDS Policy. 2002. (*Chapter 2*)

Parekh BS, Pau CP, Kennedy MS, et al. Assessment of Antibody Assays for Identifying and Distinguishing Recent from Long-Term HIV Type 1 Infection. AIDS Research and Human Retroviruses. 2001; 17:137-46. (*Chapter 5*)

Power R. The application of qualitative research methods to the study of sexually transmitted infections. Sex Transm Infect 2002; 78:87-89. (*Chapter 2*)

Schensul SL, Schensul JJ, and LeCompte MD. Essential ethnographic methods. Observations, interviews, and questionnaires. In: The Ethnographer's Toolkit (Vol 2). Walnut Creek, CA: Altamira Press, 1999. (*Chapter 2*)

Schensul JJ and LeCompte MD, eds. The Ethnographer's Toolkit (Vols.1-7). Walnut Creek, CA: Altamira Press. 2002. (For content of specific volumes, go to:
[http://www.altamirapress.com/Catalog/SingleBook.shtml?command=Search&db=^DB/CATALOG.db&eqSKUdata=0761990429&thepassedurl=\[thepassedurl\]](http://www.altamirapress.com/Catalog/SingleBook.shtml?command=Search&db=^DB/CATALOG.db&eqSKUdata=0761990429&thepassedurl=[thepassedurl])) (*Chapter 2*)

Scrimshaw SC, Carballo M, Ramos L, Blair BA. The AIDS rapid anthropological assessment procedures: a tool for health education planning and evaluation. Health Education Q 1991; 18(1):111-123. (*Chapter 2*)

Stimson, G.V., MC Donoghoe, C. Fitch and T.J. Rhodes, eds. Rapid Assessment and Response Technical Guide. WHO/HIV/2002.22. Geneva: The World Health Organization, 2002.
<http://www.who.int/docstore/hiv/Core/Contents.html>. Accessed March 1, 2007. (*Chapter 2*)

Stueve A, O'Donnell L, Duran R, et al. Time-space sampling in minority communities: Results with young Latino men who have sex with men. American Journal of Public Health 2001; 91:922-926. (*Chapters 1 and 9*)

Trotter RT, Needle RH, Goosby E; Bates C, Singer M. A methodological model for Rapid Assessment, Response, and Evaluation: The RARE Program in Public Health. Field Methods 2001; 13(2):137-159. (*Chapter 2*)

Ulin PR, Robinson ET, and Tolley EE. Qualitative methods in public health research. A Field Guide for Applied Research. Jossey-Bass, San Francisco, CA, 2005. (*Chapter 2*)

Valleroy LA, MacKellar DA, Karon JM, et al. HIV prevalence and associated risks in young men who have sex with men. JAMA 2000;284:198--204. (*Chapters 1 and 9*)

ACKNOWLEDGEMENTS

These national protocol guidelines were written by staff of the Behavioral Surveillance Team, Behavioral and Clinical Surveillance Branch (BCSB), Division of HIV/AIDS Prevention– Surveillance and Epidemiology (DHAP-SE), National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention (NCHHSTP), Centers for Disease Control and Prevention (CDC).

Because the National HIV Behavioral Surveillance System (NHBS) protocol guidelines were prepared by employees of the federal government as part of their official duties, they are part of the public domain and are not copyright protected under Title 17 of the United States Copyright Code. Accordingly, these protocol guidelines may be copied and shared with others without CDC approval.

CONTACTS

For inquiries about this protocol or NHBS, please contact the following CDC staff:

Protocol

Paul Denning, MD, MPH
Epidemiologist
Centers for Disease Control and Prevention
1600 Clifton Rd, Mailstop E-46
Atlanta, Georgia 30333
Telephone: (404) 639-2963; E-mail: pdenning@cdc.gov

Nevin Krishna MS, MPH
Epidemiologist
Centers for Disease Control and Prevention
1600 Clifton Rd, Mailstop E-46
Atlanta, Georgia 30333
Telephone: (404) 639-8666; E-mail: nkrishna1@cdc.gov

Isa J. W. Miles, ScD, MS
Behavioral Scientist
Centers for Disease Control and Prevention
1600 Clifton Rd, Mailstop E-46
Atlanta, Georgia 30333
Telephone: (404) 639-6304; E-mail: IMiles@cdc.gov

Catlainn Sionean, PhD
Behavioral Scientist
Centers for Disease Control and Prevention
1600 Clifton Rd, Mailstop E-46

Atlanta, Georgia 30333
Telephone: (404) 639-8702; E-mail: CSionean@cdc.gov

Amanda Smith, MPH
Epidemiologist
Centers for Disease Control and Prevention
1600 Clifton Rd, Mailstop E-46
Atlanta, Georgia 30333
Telephone: (404) 639-2978; E-mail: asmith3@cdc.gov

Cyprian Wejnert, PhD
Epidemiologist
Centers for Disease Control and Prevention
1600 Clifton Rd, Mailstop E-46
Atlanta, Georgia 30333
Telephone: (404) 639-6055; E-mail: cwejnert@cdc.gov

NHBS General Inquiries

Alexandra M. Oster, MD
Epidemiologist
Team Leader (Acting), Behavioral Surveillance
Centers for Disease Control and Prevention
1600 Clifton Rd, Mailstop E-46
Atlanta, Georgia 30333
Telephone: (404) 639-6141; E-mail: aoster@cdc.gov

Appendix A

Model Key Informant Interview Consent Form

English Version; Grade Reading Level by Flesch-Kincaid Method: 7.9

National HIV Behavioral Surveillance System Key Informant Consent Form

A. Purpose

The [**Agency Name**] and the Centers for Disease Control and Prevention (CDC) are doing a study of men who may be at risk for HIV infection, and who will be asked to take an HIV test. The reason for this interview is to learn about the best way to do this future study. We are asking you to participate in this interview because you may be able to provide us with ideas about the future study.

B. Procedures

If you agree to be interviewed, this is what will happen.

1. During the interview, a staff member will ask you questions about the following issues:
 - a. Ways to encourage men to take the survey;
 - b. Names of places and social organizations that are attended by men who have sex with men (MSM);
 - c. Reasons people might not want to take an HIV test, and ways to encourage them to do so;
 - d. Payment for the survey;
 - e. Descriptions of local neighborhoods and communities of persons at-risk of HIV.
2. Notes from the interview will be recorded on paper.
3. You can refuse to answer a question at any time. If you do not answer a question or want to end the interview, there will not be any penalty to you. No one except the study staff at [**Agency Name**] will have access to the information you provide to us.

The interview is anonymous. Your name will not be attached to your responses.

C. Discomforts and Risks

There are no physical risks to you by participating in this interview. No one will ask about your own behaviors, and you should not share this information during your interview.

D. Benefits

There are no direct benefits by being in this interview. The information you give us may help us have a better future study.

E. Compensation

You will not be paid for the time you spend taking part in the interview.

F. Persons to Contact

This study is run by: *[name of principal investigator and phone number]*. You may call [him/her] with any questions about being interviewed.

If you have questions about your rights as a participant or if you feel that you have been harmed, contact *[IRB committee or contact name and phone number]*.

G. Confidentiality Statement

What you tell us is confidential. No one except the study staff at **[Agency Name]** and CDC will have access to your comments, except as otherwise required by law. Any comments made by you will not be attributed to you as an individual but to the collective group of individuals we interview as a whole. This interview will not be audio- or video-taped.

H. Right to Refuse or Withdraw

Doing this interview is VOLUNTARY. You have the right to refuse to answer any questions. You can end the interview at any time you want.

I. Agreement

Do you have any questions?

Interviewer: Answer the participant's questions about the interview before proceeding to the next question.

You have read or had read to you the explanation of this study, you have been given a copy of this form, the opportunity to discuss any questions that you might have and the right to refuse participation. I am going to ask for your consent to participate in this interview. By saying yes, you agree to participate in the interview. Do you agree to take part in the interview?

Date: _____ Interviewer initials in box confirm affirmative consent

I have fully explained to the participant the nature and purpose of the procedures described above and the risks involved in its performance. I have asked if any questions have arisen regarding the procedures and have answered these questions to the best of my ability.

Date: _____ Signature of interviewer: _____

Appendix B

Model Community Key Informant Interview Consent Form

English Version; Grade Reading Level by Flesch-Kincaid Method: 7.9

National HIV Behavioral Surveillance System Community Key Informant Consent Form

A. Purpose

The [Agency Name] and the Centers for Disease Control and Prevention (CDC) are doing a study of men who may be at risk for HIV infection, and who will be asked to take an HIV test. The reason for this interview is to learn about the best way to do this future study. We are asking you to participate in this interview because you may be able to provide us with ideas about the future study.

B. Procedures

If you agree to be interviewed, this is what will happen.

1. During the interview, a staff member will ask you questions about the following issues:
 - a. Ways to encourage men to take the survey;
 - b. Names of places and social organizations that are attended by men who have sex with men (MSM);
 - c. Reasons people might not want to take an HIV test, and ways to encourage them to do so;
 - d. Payment for the survey;
 - e. Opinions that people in this neighborhood have about HIV and HIV prevention.
 - f. Descriptions of local neighborhoods and communities of persons at-risk of HIV.
2. Notes from the interview will be recorded on paper.
3. You can refuse to answer a question at any time. If you do not answer a question or want to end the interview, there will not be any penalty to you. No one except the study staff at [Agency Name] will have access to the information you provide to us.
4. The interview is anonymous. Your name will not be attached to your responses.
5. You will receive \$25.00 for the time you spend taking part in the interview.

C. Discomforts and Risks

There are no physical risks to you by participating in this interview. No one will ask about your own behaviors, and you should not share this information during your interview.

D. Benefits

There are no direct benefits by being in this interview. The information you give us may help us have a better future study.

E. Compensation

You will be paid \$25 for the time you spend taking part in the interview.

F. Persons to Contact

This study is run by: [*name of principal investigator and phone number*]. You may call [him/her] with any questions about being interviewed.

If you have questions about your rights as a participant or if you feel that you have been harmed, contact [*IRB committee or contact name and phone number*].

G. Confidentiality Statement

What you tell us is confidential. No one except the study staff at [**Agency Name**] and CDC will have access to your comments, except as otherwise required by law. Any comments made by you will not be attributed to you as an individual but to the collective group of individuals we interview as a whole. This interview will not be audio- or video-taped.

H. Right to Refuse or Withdraw

Doing this interview is VOLUNTARY. You have the right to refuse to answer any questions. You can end the interview at any time you want.

I. Agreement

Do you have any questions?

Interviewer: Answer the participant's questions about the interview before proceeding to the next question.

You have read or had read to you the explanation of this study, you have been given a copy of this form, the opportunity to discuss any questions that you might have and the right to refuse participation. I am going to ask for your consent to participate in this interview. By saying yes, you agree to participate in the interview. Do you agree to take part in the interview?

Date: _____ Interviewer initials in box confirm affirmative consent

I have fully explained to the participant the nature and purpose of the procedures described above and the risks involved in its performance. I have asked if any questions have arisen regarding the procedures and have answered these questions to the best of my ability.

Date: _____ Signature of interviewer: _____

Appendix C

Model Focus Group Consent Form

English Version; Grade Reading Level by Flesch-Kincaid Method: 7.4

National HIV Behavioral Surveillance System Focus Group Consent Form

A. Purpose

The [Agency Name] and the Centers for Disease Control and Prevention (CDC) will be doing a survey of men who may be at risk for HIV infection and who will be asked to take an HIV test. The reason for the focus group is to learn about the best way to do this future study. We are asking you to be in the group because you may be able to provide us with ideas about the future study.

B. Procedures

1. If you agree to be in the focus group, you will take part in a focus group with up to 10 other people that will last between 1 ½ and 2 hours.
2. During the session, people will be asked questions about the following issues:
 - a. Ways to encourage men to take the survey;
 - b. Names of places and social organizations that are attended by men who have sex with men (MSM);
 - c. Reasons people might not want to take an HIV test, and ways to encourage them to do so;
 - d. Payment for the survey.
3. Notes from the focus groups will be recorded on paper.
4. The focus group is anonymous. We will not record your name or any other characteristics that might identify you at any time during the interview. No one except the study staff at [Agency Name] will have access to the information you provide to us.
5. You will be given \$25.00 for being in the focus group.
6. You can refuse to answer a question at any time. If you do not answer a question or want to leave the focus group, there will not be any penalty to you.

C. Discomforts and Risks

There are no physical risks to you by participating in this focus group. No one will ask about your own behaviors, and you should not share this information during your session.

Other focus group members may say things that may make you feel uncomfortable. If this happens, the staff will help to resolve the problem.

D. Benefits

The information you give us may help us have a better future survey.

E. Compensation

You will be paid \$25 for the time you spend taking part in the focus group.

F. Persons to Contact

This focus group is run by: [name of principal investigator and phone number]. You may call [him/her] with any questions about being in the focus group.

If you have questions about your rights as a participant or if you feel that you have been harmed, contact [IRB committee or contact name and phone number].

G. Confidentiality Statement

What you tell us is confidential. Your responses will be labeled with a study number only. No one except the study staff at [Agency Name] and CDC will have access to the focus group's comments, except as otherwise required by law. Any comments made by persons in this group will not be attributed to individual members but to the group as a whole. This focus group will not be audio- or video-taped.

H. Right to Refuse or Withdraw

Being in this focus group is VOLUNTARY. You have the right to refuse to answer any questions. You can leave the focus group at any time.

I. Agreement

Do you have any questions?

Moderator: Answer the participant's questions about the focus group before proceeding to the next question.

You have read or had read to you the explanation of this study, you have been given a copy of this form, the opportunity to discuss any questions that you might have and the right to refuse participation. I am going to ask for your consent to participate in this focus group. By saying yes, you agree to participate in the focus group. Do you agree to take part in the focus group?

Date: _____ Moderator initials in box confirm affirmative consent

I have fully explained to the participant the nature and purpose of the procedures described above and the risks involved in its performance. I have asked if any questions have arisen regarding the procedures and have answered these questions to the best of my ability.

Date: _____ Signature of moderator: _____

Appendix D

Intercept Form and Instructions

Intercept Form

Venue Code: _____ Event Number: _____ Date: ____ / ____ / ____

Venue Name: _____ Recruiter: _____

#	Didn't Stop	Previously Participated	Previously Asked	Accepted Intercept	Agreed to Screening	Comments
1		Y N U	Y N U	Y N	Y N	
2		Y N U	Y N U	Y N	Y N	
3		Y N U	Y N U	Y N	Y N	
4		Y N U	Y N U	Y N	Y N	
5		Y N U	Y N U	Y N	Y N	
6		Y N U	Y N U	Y N	Y N	
7		Y N U	Y N U	Y N	Y N	
8		Y N U	Y N U	Y N	Y N	
9		Y N U	Y N U	Y N	Y N	
10		Y N U	Y N U	Y N	Y N	
11		Y N U	Y N U	Y N	Y N	
12		Y N U	Y N U	Y N	Y N	
13		Y N U	Y N U	Y N	Y N	
14		Y N U	Y N U	Y N	Y N	
15		Y N U	Y N U	Y N	Y N	
16		Y N U	Y N U	Y N	Y N	
17		Y N U	Y N U	Y N	Y N	
18		Y N U	Y N U	Y N	Y N	
19		Y N U	Y N U	Y N	Y N	
20		Y N U	Y N U	Y N	Y N	
						← Sub-totals

Page (circle one): 1 2 3 4 5 of ____

Overview

Recruiters should record all information collected during an intercept on the Intercept Form. Project sites may customize the Intercept Form to meet their own needs, but if they do, they must include all the data elements collected on the model form provided by CDC. Instructions for completing the Intercept Form are outlined below.

Recruitment Event Information

Information needed to identify the recruitment event is collected at the top of the Intercept Form. To help keep track of forms, recruiters should enter the required information on all forms used during the recruitment event, not just on the first form.

Description of the recruitment event information

Venue Code: The 4-digit venue identification code assigned to the venue where the recruitment event is being conducted.

Venue Name: The name of the venue where the recruitment event is being conducted.

Event Number: The consecutive number assigned to the recruitment event. Each recruitment event must have its own unique number.

Date: The date of the recruitment event in a month/day/year format. If an event runs over two days (e.g., starts at 10:00 PM one day and ends at 2:00 AM the next), project sites should record the date the event began.

Recruiter: The recruiter's name or, if a project site prefers, the recruiter's identification code. Each recruiter working at a recruitment event must have their own Intercept Form(s).

Recruitment Data

Each numbered line on the Intercept Form represents recruitment data on a different venue attendee approached to participate in NHBS-MSM3. To ensure that recruitment data are accurate, recruiters must make an entry on the Intercept Form for every venue attendee they attempt to intercept, even if the attendee ignores them and does not stop.

Description of the recruitment data

(Number): A running count of the venue attendees approached to participate in NHBS-MSM3. The first attendee approached by the recruiter is number 1, the second attendee approached is number 2, and so on. The recruiter should consecutively circle the numbers on the

form when they approach venue attendees for recruitment.

Didn't Stop: If a recruiter attempts to intercept a venue attendee and the attendee ignores them or does not stop, the recruiter should check "Didn't Stop." The recruiter should also check "Didn't Stop" if the attendee stops, but refuses to answer both recruiter questions ("Previously Participated" and "Previously Asked" below). When a recruiter checks "Didn't Stop" for a venue attendee, they do not need to record any other recruitment data on the attendee. Nevertheless, if the venue attendee provides a reason why he is not interested in participating in the survey, the recruiter should note this in the "comments" field.

Previously Participated: After a recruiter intercepts a venue attendee and greets him, they should ask the first recruiter question:

During 2011, did you complete at least part of the health survey that (project name or sponsoring agency's name) is conducting? It could have been here or at another location.

Based on the venue attendee's response, the recruiter should circle either the "Y" (yes), "N" (no), or "U" (unsure) in the "Previously Participated" field:

Venue Attendee's Response	Letter to Circle
Indicates that he completed at least part of the survey during the current project cycle. (This includes men who were found to be ineligible or stopped the survey prematurely.)	Y
Indicates that he did not complete any of the survey during the current project cycle.	N
Indicates that he is unsure whether he completed any of the survey during the current project cycle.	U
Does not answer or refuses to answer.	None

If the attendee already completed at least part of the survey ("Y" [yes] response), the recruiter should thank him for helping with the project and the recruiter should end the intercept. For all other attendees, the recruiter should continue the intercept.

Previously Asked: If the venue attendee does not indicate that he completed at least part of the survey, the recruiter should ask the second recruiter question:

During 2011, did anyone approach you like I did and ask you to participate in the health survey that (project name or sponsoring agency's name) is conducting? It could have been here or at another location.

Based on the venue attendee's response, the recruiter should circle either the "Y" (yes), "N" (no),

or “U” (unsure) in the “Previously Asked” field:

Venue Attendee's Response	Letter to Circle
Indicates that he was previously asked to participate in the survey during the current project cycle.	Y
Indicates that he was not previously asked to participate in the survey during the current project cycle.	N
Indicates that he is unsure whether he was previously asked to participate in the survey during the current project cycle.	U
Does not answer or refuses to answer.	None

Accepted Intercept: The recruiter must record a response in the “Accepted Intercept” field for all venue attendees they approach, including those who did not stop to answer the two recruiter questions. Based on the entries in the “Didn’t Stop,” “Previously Participated,” and “Previously Asked” fields, the recruiter should circle either the “Y” (yes) or “N” (no) in the “Accepted Intercept” field.

The recruiter should circle the “Y” if:

- the “Y” is circled for “Previously Participated”

OR

- the “N” or “U” is circled for "Previously Participated" **and** the “Y,” “N,” or “U” is circled for “Previously Asked.”

The recruiter should circle the “N” if:

- “Didn’t Stop” is checked

OR

- the venue attendee refused to answer **either** of the recruiter questions.

Agreed to Screening: As described in Chapter 4, venue attendees who have not previously participated in NHBS-MSM3 should be invited to participate in the survey. If the attendee agrees to be screened for NHBS-MSM3 eligibility, the recruiter should circle the “Y” (yes) in the “Agreed to Screening” field, and if the attendee does not agree to be screened, the recruiter should circle the “N” (no).

Comments: The recruiter can use the “Comments” field to record any additional information

provided by the venue attendees they approach, such as reasons for refusing to accept the intercept or for declining to participate in the survey. Project sites can use this information to identify any potential barriers to recruitment or participation.

Page Numbers

To help keep track of the Intercept Forms, the recruiter should number the forms they have used during a recruitment event. The bottom of the form has a field for the recruiter to circle the page number and indicate the total number of forms they used.

Data Summation

At the end of a recruitment event, the Field Supervisor should collect all the Intercept Forms used during the event. They should then tabulate the number of venue attendees approached and the number of “Y” (yes) responses recorded in each column on the form. The columns that need to be tabulated on the Intercept Form have been shaded and the bottom of the form has a line to record the column sub-totals. Once the Field Supervisor has calculated the column sub-totals on each form, they should add them together to calculate totals for the recruitment event. Event-level data will then be submitted to the CDC and DCC.

Tabulating column sub-totals

Number of Venue Attendees Approached: The highest number circled in the “#” (number) field. For example, if numbers 1 through 12 were circled, the number of venue attendees approached would be 12.

Number of Venue Attendees Who Previously Participated: The number of “Y” (yes) responses circled in the “Previously Participated” field.

Number of Venue Attendees Who Were Previously Asked to Participate: The number of “Y” (yes) responses circled in the “Previously Asked” field.

Number of Venue Attendees Who Accepted the Intercept: The number of “Y” (yes) responses circled in the “Accepted Intercept” field.

Number of Venue Attendees Who Agreed to Screening: The number of “Y” (yes) responses circled in the “Agreed to Screening” field.

Form Approved:
OMB No. XXXX-XXXX
Expiration Date: XX/XX/XXXX

National HIV Behavioral Surveillance System: Eligibility Screener

Public reporting burden of this collection of information is estimated to average 5 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a currently valid OMB control number. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to: CDC, Project Clearance Officer, 1600 Clifton Road, MS D-74, Atlanta, GA 30333, ATTN: PRA (XXXX-XXXX). Do not send the completed form to this address.

National HIV Behavioral Surveillance System: Eligibility Screener

AUTO1. NHBS Round ____

AUTO2. NHBS Cycle ____ (1=MSM; 2=IDU; 3=HET)

AUTO3 Date of Interview: ____/____/_____
(M M / D D / Y Y Y Y)

AUTO4. Time Begin ____:____ 1AM 2PM

AUTO5. Version _____

Interviewer Entered Information

INT1. *Interviewer ID* ____

INT2. *Enter City* ____

INT3. *Survey ID* _____

*If the length of Survey ID is 4 digits and Cycle=1 skip to INT4;
If the Length of Survey ID is 4 digits and Cycle=2 or 3 skip to INT9.*

CONF1. **Interviewer:** The survey ID that you entered was [INT3]. Is this correct?
 No..... 0 *Loop back to INT3*
 Yes..... 1

If NHBS-IDU or NHBS-HET (CYCLE=2 or 3), skip to INT9.

INT4. *Venue ID* _____

INT5. *Event Number* _____

INT6. **Interviewer:** Is this interview an “Other Day Appointment”?
 No..... 0 *Skip to Say Box before ES1*
 Yes..... 1

Other Day Appointment

INT7. *Enter the field site ID for the location of the interview:* _____

INT8. *Enter the date of the recruitment event:* _____ / _____ / _____
 M M / D D / Y Y Y Y

If NHBS-MSM (CYCLE=)1, skip to Say Box before ES1.

INT9. **Field Site ID** ___ ___

CONF2. **Interviewer:** The field site ID that you entered was [*Response to INT9*]. Is this correct?
No..... 0 **Loop back to INT9**
Yes..... 1

INT10. **Interviewer:** Is participant a seed?
No..... 0
Yes..... 1

FOR ALL NHBS CYCLES

SAY: I'd like to thank you again for your interest in this health survey. Remember that all information you give me will be kept private and I will not ask for your name. First, I will ask you a few questions about yourself and then the computer will determine if you have been selected to participate in the health survey.

Eligibility Screener Questions

ES1. What is your date of birth?

[Refused = 77/7777, Don't know = 99/9999] (M M / D D / Y Y Y Y)

**So, you are [insert calculated age] years old. Is that correct?
If Respondent is <18 years old, skip to End1**

ES2. During 20xx, did you already complete at least part of the health survey that [*Insert Project Name*] is conducting? It could have been here or at another location.
No..... 0
Yes..... 1
Known previous participant..... 2
Refused to answer..... 7
Don't know..... 9

ES3. Do you consider yourself to be Hispanic or Latino/a? **[Interviewer: If necessary, say “Just tell me Yes or No.”]**

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

If ES3 in (0, 7, 9), skip to ES4.

ES3a. What best describes your Hispanic or Latino ancestry?
[READ CHOICES. CHECK ALL that apply.]

- Mexican..... 1
- Puerto Rican..... 2
- Cuban..... 3
- Dominican..... 4
- Other (*Specify*.....)..... 5
- Refused to answer..... 7
- Don't know..... 9

ES4. **[GIVE RESPONDENT FLASHCARD A.]** Which racial group or groups do you consider yourself to be in? You may choose more than one option. **[READ CHOICES. CHECK ALL THAT APPLY.]**

- American Indian or Alaska Native..... 1
- Asian..... 2
- Black or African American..... 3
- Native Hawaiian or Other Pacific Islander..... 4
- White..... 5
- Refused to answer..... 7
- Does not apply..... 8
- Don't know..... 9

ES5. What county do you currently live in? _____
(List of eligible counties on computer)

If “Other” county chosen, specify, then skip to Logic check before ES6.

ES5a. How long have you been living in [*project area*]? (*Interviewer*: If response is in months, enter 0 below and then enter the number of months in the next screen.)

Years __ __

[*Refused = 777, Don't know = 999*]

If ES5a= 1-100, 777, or 999, skip to Logic Check before ES6

ES5b. **Number of months:** __ __
range of values= 1-11

[*Refused = 77, Don't know = 99*]

For NHBS-MSM, skip to ES8
For NHBS-IDU, skip to ES9
For NHBS-HET, ask ES6 - ES7a, then skip to ES9

ES6. What zip code do you live in?

[*Refused = 77777, Don't know = 99999*] _ _ _ _ _

ES7. **SHOW RESPONDENT THE MAP** (*example provided at end of this document*)
Please take a look at this map. Can you point to the area where you live?

Interviewer: Enter 6-digit census tract # _____
(*Refused= 777777, Don't know= 999999*)

ES7a. IF RESPONDENT IS A SEED (INT10=1)
Interviewer: Does participant live in a High Risk Area?
No 0
Yes 1

Skip to ES9

FOR NHBS-MSM

ES8. What was your sex at birth? [**CHECK only ONE**]

Male..... 1
Female..... 2
Intersex/ambiguous..... 3
Refused to answer..... 7
Don't know..... 9

FOR ALL NHBS CYCLES

ES9. Do you consider yourself to be male, female, or transgender? [*CHECK only ONE*]

- Male..... 1
- Female..... 2
- Transgender..... 3
- Refused to answer..... 7
- Don't know..... 9

If NHBS-IDU skip to ES10. If NHBS-HET, skip to Logic check before ES17.

NHBS-MSM behavioral eligibility questions

ES9a. Have you ever had vaginal or anal sex with a woman?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

ES9b. Have you ever had oral or anal sex with a man?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

FOR NHBS-MSM, skip to SAY Box before ES18
FOR NHBS-IDU, ask ES10 - ES17b, then skip to SAY Box before ES18
FOR NHBS-HET, skip to Logic Check before ES17

NHBS-IDU behavioral eligibility screener questions

ES10. Have you ever in your life shot up or injected any drugs other than those prescribed for you? By shooting up, I mean anytime you might have used drugs with a needle, either by mainlining, skin popping, or muscling.

- No..... 0 → *Skip to SAY box before ES18*
- Yes..... 1
- Refused to answer..... 7 } *Skip to SAY box before ES18*
- Don't know..... 9 }

ES11. When was the last time you injected any drug? That is, how many days or months or years ago did you last inject? *[Interviewer: Enter the number below. If today, enter 0]*

Number
[Refused = 777, Don't know = 999]

If ES11 in (777, 999), skip to ES12.

ES11a. *Interviewer:* Was this days or months or years? *[If today, enter “days”]*

- Days..... 1
- Months..... 2
- Years..... 3

ES12. Which drug do you inject most often? *[READ CHOICES. CHECK ONLY ONE]*

- Speedball – Heroin and cocaine together 1
- Heroin, by itself..... 2
- Cocaine, by itself..... 3
- Crack..... 4
- Crystal, meth, tina, crank, ice..... 5
- Something else (*Specify*_____). 6
- Refused to answer..... 7
- Don't know..... 9

ES13. Where on your body do you usually inject? [**CHECK ALL THAT APPLY**]
[Interviewer: Have participant show ALL injection areas on body. Check for physical signs of injection]

- Fresh track marks..... 1
- Needle-sized scabs..... 2
- Abscesses..... 3
- Old track marks or scars..... 4
- Injects in covered area 5
- No physical signs..... 6
- Respondent refused to show..... 7

If participant has no visible physical signs of current injection, ask ES14-ES16. Otherwise, go to SAY Box before ES18.

ES14. Step-by-step, tell me how you prepare your drugs.

INTERVIEWER:
Description could include:
Mix drugs with water or lemon juice/vinegar
Use cooker /Heat drugs
Use filter
Description OK..... 1
Description Not OK..... 2

ES15. Step-by-step, tell me how you inject your drugs.

INTERVIEWER:
Description could include:
Tie off and find vein (IVDU)
Clean injection site
Register (IVDU)
Description OK..... 1
Description Not OK..... 2

ES16. What type of syringe do you usually inject with?

INTERVIEWER:
Description could include:
Syringe size (in cc's or units)
Needle size (gauge, length)
Cap (color, number)

(Can also ask where they usually get syringes, what they do with them after injecting, and how they know if they are new or used)

Description OK..... 1
Description Not OK..... 2

If NHBS-IDU, skip to SAY Box before ES18

IF ES9 is not 1 (male) or 2 (female), then skip to ES17c.

NHBS-HET behavioral eligibility questions

SAY: The next questions are about having sex. Please remember your answers will be kept private.

ES17. Have you had sex with a *[insert “man” if respondent is female; insert “woman” if respondent is male]* in the past 12 months?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

If ES17 is not 1, skip to SAY box before ES18.

ES17a. Did you have vaginal sex? By vaginal sex, I mean *[insert “he put his penis in your vagina” if respondent is female; insert “you put your penis in her vagina” if respondent is male]*.

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

If ES17a = 1, skip to SAY box before ES18.

ES17b. Did you have anal sex? By anal sex, I mean *[insert “he put his penis in your anus (butt)” if respondent is female; insert “you put your penis in her anus (butt)” if respondent is male]*

- No..... 0
Yes..... 1
Refused to answer..... 7
Don't know..... 9

If ES17b = 1, skip to SAY box before ES18.

CONF3. Ask the following if ES17=1 AND ES17a=0 AND ES17b=0):

“So, in the last 12 months, you only had oral sex with a *[insert “man” if respondent is female; insert “woman” if respondent is male]*? Is that correct?

If NOT correct, go back to ES17a.

If CORRECT, go to SAY box before ES18.

ES17c. Have you had sex in the past 12 months?

- No..... 0
Yes..... 1
Refused to answer..... 7
Don't know..... 9

SAY: We’ve finished the first series of questions. Now the computer will determine whether you’ve been selected to participate in the survey.

FOR ALL NHBS CYCLES

ES18. **Interviewer:** Is this person alert and able to complete the health survey in English or Spanish?

- No..... 0
Yes..... 1

If ES18=0 and NHBS-MSM or NHBS-IDU, display ES18a; then, go to End1.

If ES18=0 and NHBS-HET, display interviewer instruction ES18b; then go to End1.

ES18a. **Interviewer:** Specify reason person not able to complete the interview:

- Not alert..... 1
- Not able to complete in English or Spanish..... 2
- Thought to be too young..... 3
- Other (specify _____)..... 4

ES18b. **Interviewer:** Specify reason person not able to complete the interview:

- Not alert..... 1
- Not able to complete in English or Spanish..... 2
- Thought to be too young..... 3
- Thought to be too old..... 4
- Other (specify _____)..... 5

AUTO6. Time Eligibility Screener Ended: ___:___:___ [Military time HH:MM:SS]

Eligibility is calculated based on cycle-specific eligibility criteria defined in the protocol

End 1. If the participant IS NOT ELIGIBLE:

SAY: Thank you for answering these questions. Unfortunately, the computer has not selected you to participate in the health survey. Thank you again for your time.

End Interview.

End 2. If the participant IS ELIGIBLE:

SAY: Congratulations! The computer has selected you to participate in the health survey. Let me tell you about it. ***Interviewer: Proceed with the consent process.***

Interviewer: Conduct the local IRB-approved consent process

- CN-1. Do you agree to take part in the survey?
- No..... 0
 - Yes..... 1

If CN-1 = 0, display: Thank the respondent for doing the eligibility screener. Then skip to CN-5.

- CN-2. Do you agree to HIV counseling and testing?
- No..... 0
- Yes..... 1

If CN-2=0, display:

Interviewer: You have documented that the person DID NOT consent to HIV counseling and testing. If the person DID consent to HIV testing, please arrow back and re-enter the consent for HIV testing.

If interviewer confirms CN-2=0, and NHBS-MSM, skip to NHBS-MSM Core Intro.

If interviewer confirms CN-2=0, and NHBS-IDU, skip to NHBS-IDU Core Intro.

If interviewer confirms CN-2=0 and NHBS-HET, skip to NHBS-HET Core Intro.

- CN-3. Do you agree to have other lab tests (if offered)?
- No..... 0
- Yes..... 1
- Does not apply..... 8

- CN-4. Do you agree to let us store a sample of your blood for future testing?
- No..... 0
- Yes..... 1
- Does not apply..... 8

If NHBS-MSM, skip to NHBS-MSM Core Intro.

If NHBS-IDU, skip to NHBS-IDU Core Intro.

If NHBS-HET, skip to NHBS-HET Core Intro.

- CN-5. We're interested in knowing why people do not want to do this study. Would you mind telling me which of the following best describes the reason you do not want to do this study?
[READ CHOICES. CHECK ALL THAT APPLY.]
- You don't have time..... 1
- You don't want to talk about these topics..... 2
- Some other reason..... 3
- You'd rather not say why..... 9

Form Approved:
OMB No. XXXX-XXXX
Expiration Date: XX/XX/XXXX

National HIV Behavioral Surveillance System: Core Questionnaire

MSM Cycle

Public reporting burden of this collection of information is estimated to average **XX** minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a currently valid OMB control number. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to: CDC, Project Clearance Officer, 1600 Clifton Road, MS D-74, Atlanta, GA 30333, ATTN: PRA (**XXXX-XXXX**). Do not send the completed form to this address.

Form Approved:
OMB No. XXXX-XXXX
Expiration Date: XX/XX/XXXX

National HIV Behavioral Surveillance System: Core Questionnaire

IDU Cycle

Public reporting burden of this collection of information is estimated to average **XX** minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a currently valid OMB control number. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to: CDC, Project Clearance Officer, 1600 Clifton Road, MS D-74, Atlanta, GA 30333, ATTN: PRA (**XXXX-XXXX**). Do not send the completed form to this address.

Form Approved:
OMB No. XXXX-XXXX
Expiration Date: XX/XX/XXXX

National HIV Behavioral Surveillance System: Core Questionnaire

HET Cycle

Public reporting burden of this collection of information is estimated to average **XX** minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a currently valid OMB control number. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to: CDC, Project Clearance Officer, 1600 Clifton Road, MS D-74, Atlanta, GA 30333, ATTN: PRA (**XXXX-XXXX**). Do not send the completed form to this address.

National HIV Behavioral Surveillance System: Core Questionnaire

AUTO7. Time core questionnaire began: __ __: __ __: __ __ [Military time HH:MM:SS]

NHBS-MSM Core Intro:

SAY: “Most people have never been in an interview like this one, so I’m going to describe how it works before we start. I will read you questions exactly as they are written. Some may sound awkward but I need to read them as worded so everyone in the study is asked the same questions. Some questions will ask you to recall if you did something, when you did it, or how often you did it. For others, I’ll read or show you a list of responses to choose from. Please be as accurate as you can.”

Go to Say Box before DM-1

NHBS-IDU Core Intro:

SAY: “Most people have never been in an interview like this one, so I’m going to describe how it works before we start. I will read you questions exactly as they are written. Some may sound awkward but I need to read them as worded so everyone in the study is asked the same questions. Some questions will ask you to recall if you did something, when you did it, or how often you did it. For others, I’ll read or show you a list of responses to choose from. Please be as accurate as you can.”

If R is NOT a seed (INT10=0), SAY:

“I’m going to start by asking you about the person who gave you this coupon and about other people you know in [*project area*] who inject. Please remember that your answers will be kept private.” [**Go to NS-1.**]

Else, if R IS a seed (INT10=1), Go to NS-2

NHBS-HET Core Intro:

SAY: “Most people have never been in an interview like this one, so I’m going to describe how it works before we start. I will read you questions exactly as they are written. Some may sound awkward but I need to read them as worded so everyone in the study is asked the same questions. Some questions will ask you to recall if you did something, when you did it, or how often you did it. For others, I’ll read or show you a list of responses to choose from. Please be as accurate as you can.”

If R is NOT a seed (INT10=0), SAY:

“I’m going to start by asking you about the person who gave you this coupon and about other people you know in [*Response to INT2*] who you are close to. Please remember that your answers will be kept private.” [**Go to NS-1a.**]

Else, if R IS a seed (INT10=1), Go to NS-3

Recruiter Relationship, NHBS-IDU

NS-1. **[GIVE RESPONDENT FLASHCARD B.1.]** Which of the following describes how you know the person who gave you this coupon? You can choose more than one answer. **[READ CHOICES. CHECK ALL THAT APPLY.]**

- A relative or family member 1
- A person you have sex with..... 2
- A person you use drugs with or buy drugs from 3
- A friend..... 4
- An acquaintance (that is, a person you know,
but do not consider a friend)..... 5
- A stranger (you don't know the person/just met them... 6
- Refused to answer..... 77

If NS-1 ≠ 6, go to NS-2. Else, go to CONF4.

Recruiter Relationship, NHBS-HET

NS-1a. **[GIVE RESPONDENT FLASHCARD B.2.]** Which of the following describes how you know the person who gave you this coupon? You can choose more than one answer. **[READ CHOICES. CHECK ALL THAT APPLY.]**

- A relative or family member..... 1
- A person you have sex with..... 2
- A friend 3
- An acquaintance (that is, a person you know,
but do not consider a friend)..... 4
- A stranger (you don't know the person/just met them... 5
- Refused to answer..... 77

If NS-1a ≠ 5, go to NS-3. Else, go to CONF4.

CONF4. Confirmation Message if recruiter = stranger:

IF NS-1 = 6 or NS-1a=5,
Where and when did you first see this person?

Interviewer:

If the respondent indicates that they first saw the recruiter in a situation related to the project (e.g. receiving their coupon, waiting outside the storefront, etc.), then check "Recruiter is a stranger."

NS-2a. Of the _____ *[insert number from NS-2]* people who live in *[insert project area]* and you know inject, how many have you seen at least once in the past 30 days? (Again, by “know,” I mean you know their name **OR** you see them around, even if you don’t know their name.)

[Refused= 7777, Don’t Know= 9999] ___ ___ ___

If NS-2a = 0:	Go to CONF7.
Otherwise:	Go to logic check before NS-2b.

CONF7. If R has seen NO injectors he knows in past 30 days (NS-2 = 0),	
ASK: “You said you don’t know anyone in <i>[project area]</i> who injects and who you’ve seen at least once in the past 30 days. Is this correct? Remember, by ‘know,’ I mean you know their name OR you see them around even if you don’t know their name.”	
If “NO” (respondent <u>has</u> seen an injector):	Go back to NS-2a -Enter the correct network size. -Then, go to Logic check before NS-2b
If “YES” (respondent has <u>NOT</u> seen an injector):	Go to Say Box before DM-1

If NS-2a is (0, 7777, or 9999), skip to Say Box before DM-1.
If NS-2a = 1, skip to NS-2i.

NS-2b. Of the _____ *[insert number from NS-2a]* people who inject that you have seen in the past 30 days, how many are male?

[Refused= 7777, Don’t Know= 9999] ___ ___ ___

CONF8. If NS-2b = NS-2a,
SAY: “So, all the people you know who inject and that you have seen in the past 30 days are male?”
If correct, go to SAY Box before NS-2d
If NOT correct, display interviewer instruction: SAY: “Please confirm the number of people you know who inject, who are at least 18 years old, live in <i>[project area]</i> , and that you have seen in the past 30 days.”
Then, go to NS-2a.

NS-2c. Of the _____ *[insert number from NS-2a]* people who inject that you have seen in the past 30 days, how many are female?

[Refused= 7777, Don’t Know= 9999] ___ ___ ___

SAY: What is the race or ethnic background of the __ *[insert number from NS-2a]* people who inject that you have seen in the past 30 days? That is, how many were Black, Hispanic, white, or another race?

NS-2d. How many were Black? *[Refused= 7777, Don't Know= 9999]* ___ ___ ___

NS-2e. How many were Hispanic? *[Refused= 7777, Don't Know= 9999]* ___ ___ ___

NS-2f. How many were white? *[Refused= 7777, Don't Know= 9999]* ___ ___ ___

NS-2g. How many were another race? *[Refused= 7777, Don't Know= 9999]* ___ ___ ___

Skip to SAY Box before DM-1.

Single IDU Known

NS-2h. Have you seen this person at least once in the past 30 days?

No..... 0

Yes..... 1

Refused to answer..... 7

Don't know..... 9

NS-2i. Is this person male or female?

Male..... 1

Female..... 2

Refused to answer..... 7

Don't know..... 9

NS-2j. Is *[insert "his" if NS-2i=1; insert "her" if NS-2i=2; insert "this person's" if NS-2i in (7, 9)]* Black, Hispanic, white, or another race?

Black..... 1

Hispanic..... 2

White..... 3

Another race..... 4

Refused to answer..... 7

Don't know..... 9

Skip to Say Box before DM-1.

Network Size – NHBS-HET

NS-3. Please tell me how many friends, relatives or people you are close to who are at least 18 years old, and live in *[project area]*. *[GIVE RESPONDENT FLASHCARD C.]*

[Refused= 7777, Don't Know= 9999] ___ ___ ___

IF NS-3 > 3 AND NS-3 < 7777: Go to NS-3a.
IF NS-3 = 0: Go to CONF9.
IF NS-3 > 0 AND NS-3 < 4: Go to CONF10.
If NS-3 = 7777 or 9999: Skip to Say Box before DM-1

CONF9. *Confirmation Message if overall network size = 0:*

IF NS-3 = 0,

ASK: “You said you don’t have ANY friends, relatives, or people you are close to who are at least 18 years old and live in *[project area]*. Is this correct?”

If ‘No’: (DOES know someone) go back to NS-3 (ask it again)
If ‘Yes’: (Does NOT know someone) go to Say Box before DM-1.

CONF10. *Confirmation Message if overall network size = 1, 2, or 3:*

IF NS-3 = 1, 2, OR 3

ASK: “Do you have ANY OTHER friends, relatives, or people you are close to who are at least 18 years old and live in *[project area]*?”

If ‘NO,’: Go to Logic Check before NS-3a

If ‘YES’: Go back to NS-3
-Ask it again, if needed
-Enter the correct network size.
-Then, go to Logic Check before NS-3a.

If confirmed overall network size = 1, skip to NS-3h.

NS-3a. Of those _____ *[insert number from NS-3]* people, how many have you seen at least once in the past 30 days?

[Refused= 7777, Don't Know= 9999] ___ ___ ___

SAY: What is the race or ethnic background of the __ *[insert number from NS-3a]* people that you have seen in the past 30 days? That is, how many were Black, Hispanic, white, or another race?

- NS-3d. How many are Black? *[Refused= 7777, Don't Know= 9999]* ___ ___ ___
- NS-3e. How many are Hispanic? *[Refused= 7777, Don't Know= 9999]* ___ ___ ___
- NS-3f. How many are white? *[Refused= 7777, Don't Know= 9999]* ___ ___ ___
- NS-3g. How many are another race? *[Refused= 7777, Don't Know= 9999]* ___ ___ ___

Skip to Say Box before DM-1.

Single HET Known

NS-3h. Have you seen this person at least once in the past 30 days?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

NS-3i. Is this person male or female?

- Male..... 1
- Female..... 2
- Refused to answer..... 7
- Don't know..... 9

NS-3j. Is *{insert 'he' if NS3i=1; insert 'she' if NS-3i=2; insert 'this person' if NS-3i = 7 or 9}* Black, Hispanic, white, or another race?

- Black..... 1
- Hispanic..... 2
- White..... 3
- Another race..... 4
- Refused to answer..... 7
- Don't know..... 9

National HIV Behavioral Surveillance System: Core Questionnaire

Demographics (DM)

SAY: [If NHBS-MSM, insert "I'd like to start by asking"; otherwise, insert "Next, I'd like to ask you"] some questions about where you live. Please remember your answers will be kept private."

DM-1. In the past 12 months, have you been homeless at any time? By homeless, I mean you were living on the street, in a shelter, in a Single Room Occupancy hotel (SRO), or in a car.

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

If NHBS-MSM or NHBS-IDU and DM-1 in (0, 7, 9), skip to DM-2.

If NHBS-HET and DM-1 in (0, 7, 9), skip to DM-3.

DM-1a. Are you currently homeless?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

If NHBS-HET, skip to DM-3.

DM-2. What zip code do you live in?
[Refused = 77777, Don't know = 99999] _ _ _ _ _

DM-3. Next, I would like to ask you some questions about your background. What country were you born in? *[DO NOT read choices. Check only ONE.]*

- United States..... 1
- Mexico..... 2
- Puerto Rico..... 3
- Cuba..... 4
- Other (*Specify* _____)..... 5
- Refused to answer..... 77
- Don't know..... 99

For NHBS-MSM:

If DM-3 in (1, 77, 99), skip to DM-5.

If CITY= San Juan, PR, and DM3=3, skip to DM-5.

For NHBS-IDU and NHBS-HET:

If DM-3 in (1, 77, 99), skip to DM-4.

If CITY= San Juan, PR, and DM3=3, skip to DM-4.

DM-3a. What year did you first come to live in the United States?

[7777 = Refused, 9999 = Don't know]

(Y Y Y Y)

DM-3b. What language are you most comfortable using with your family and friends? **[DO NOT READ CHOICES. CHECK ONLY ONE.]**

- English..... 1
- Spanish 2
- Chinese..... 3
- Tagalog 4
- Korean 5
- Portuguese..... 6
- Other (*Specify:* _____) 7
- Refused to answer..... 77
- Don't know 99

For NHBS-MSM, skip to DM-5

For NHBS-IDU AND NHBS-HET, ask DM-4 through DM-4a

DM-4. **[GIVE RESPONDENT FLASHCARD D.]** What is your current marital status?
[READ CHOICES. CHECK only ONE.]

- Married..... 1
- Living together as married..... 2
- Separated..... 3
- Divorced..... 4
- Widowed..... 5
- Never married..... 6
- Refused to answer..... 7
- Don't know..... 9

If DM-4= 2, ask DM-4a. Otherwise, skip to DM-5.

DM-a. Is your formal marital status separated, divorced, widowed, or never married?

- Separated..... 1
- Divorced..... 2
- Widowed..... 3
- Never married..... 4
- Refused to answer..... 7
- Don't know..... 9

DM-5. What is the highest level of education you completed?
[DO NOT read choices. Check only ONE.]

- Never attended school..... 00
- Grades 1 through 8..... 01
- Grades 9 through 11..... 02
- Grades 12 or GED..... 03
- Some college, Associate's Degree, or Technical Degree..... 04
- Bachelor's Degree..... 05
- Any post graduate studies..... 06
- Refused to answer..... 77
- Don't know..... 99

DM-6. What best describes your employment status? Are you: **[READ CHOICES. CHECK only ONE.]**

- Employed full-time..... 01
- Employed part-time..... 02
- A homemaker..... 03
- A full-time student..... 04
- Retired..... 05
- Unable to work for health reasons..... 06
- Unemployed..... 07
- Other..... 08
- Refused to answer..... 77
- Don't know..... 99

For Respondents who are not currently homeless (DM-1=0 OR DM-1a=0): Say: Next I'd like to ask you some questions about your household income. By "household income," I mean the total amount of money earned and shared by all people living in your household.

For Respondents who are currently homeless (DM-1a=1):
 Say: Next I'd like to ask you some questions about your income. By "income," I mean the total amount of money you earn or receive. This includes money other people share with you.

DM-7. What was your *[insert household income if DM-1=0 OR DM-1a=0; insert income if DM-1a=1]* last year from all sources before taxes?

GIVE RESPONDENT FLASHCARD E. DO NOT read choices.

SAY: Please take a look at this card and tell me the letter that best corresponds to your monthly or yearly income.

Monthly Income	Yearly Income	
a. 0 to \$417.....	a. 0 to \$4,999.....	<input type="checkbox"/> 00
b. \$418 to \$833.....	b. \$5,000 to \$9,999.....	<input type="checkbox"/> 01
c. \$834 to \$1041.....	c. \$10,000 to \$12,499.....	<input type="checkbox"/> 02
d. \$1042 to \$1250.....	d. \$12,500 to \$14,999.....	<input type="checkbox"/> 03
e. \$1251 to \$1667.....	e. \$15,000 to \$19,999.....	<input type="checkbox"/> 04
f. \$1668 to \$2082.....	f. \$20,000 to \$24,999.....	<input type="checkbox"/> 05
g. \$2083 to \$2500.....	g. \$25,000 to \$29,999.....	<input type="checkbox"/> 06
h. \$2501 to \$2916.....	h. \$30,000 to \$34,999.....	<input type="checkbox"/> 07
i. \$2917 to \$3333.....	i. \$35,000 to \$39,999.....	<input type="checkbox"/> 08
j. \$3334 to \$4167.....	j. \$40,000 to \$49,999.....	<input type="checkbox"/> 09
k. \$4168 to \$4999.....	k. \$50,000 to \$59,999.....	<input type="checkbox"/> 10
l. \$5000 to \$6,250.....	l. \$60,000 to \$74,999.....	<input type="checkbox"/> 11
m. \$6251 or more.....	m. \$75,000 or more.....	<input type="checkbox"/> 12
Refused to answer.....		<input type="checkbox"/> 77
Don't know.....		<input type="checkbox"/> 99

} Skip to DM-8

DM-7a. Including yourself, how many people depended on this income? **[MUST BE AT LEAST 1.]**

[Refused = 77, Don't know = 99] ___

SAY: The next questions are about health insurance. By health insurance, we mean health plans people get through employment or purchased directly as well as government programs like Medicare and Medicaid that provide medical care or help pay medical bills.

DM-8. Do you currently have health insurance or health care coverage?

- No..... 0 *Skip to DM-8b*
 Yes..... 1
 Refused to answer..... 7 } *Skip to DM-8b*
 Don't know..... 9 }

DM-8a. *[Give participant Flashcard F.]* What kind of health insurance or coverage do you currently have? *[READ choices. Check ALL that apply.]*

- A private health plan (through an employer or purchased directly) 01
 Medicaid / *[local Medicaid name]* (for people with low incomes)..... 02
 Medicare (for the elderly and people with disabilities)..... 03
 Some other government plan / *[local non-Medicaid name]*..... 04
 TRICARE (CHAMPUS)..... 05
 Veterans Administration coverage..... 06
 Some other health care plan..... 07
(Specify _____)
 Refused to answer..... 77
 Don't know..... 99

DM-8b. Is there a place that you **usually** go when you are sick or you need advice about your health?

- No..... 0
 Yes..... 1
 Refused to answer..... 7
 Don't know..... 9

If DM-8b=1, 7, or 9, skip to DM-8c.

DM-8b.1. Is this because there is no place you go for health care or because there is more than one place?

- There is **no** place..... 1
- There is **more than one** place..... 2
- Refused to answer..... 7
- Don't know..... 9

If DM-8b.1 =1, 7, or 9, skip to DM-9.

DM-8c. What kind of place [if DM-8b=1, fill "is it?"; else fill "do you go to most often"] - a clinic, doctor's office, emergency room, or some other place?

- Clinic or health center..... 1
- Doctor's office or HMO..... 2
- Hospital emergency room..... 3
- Some other place..... 4
- Doesn't go to one place most often..... 5
- Refused to answer..... 7
- Don't know..... 9

Skip to DM-9.

DM-9. Have you seen a doctor, nurse, or other health care provider in the past 12 months?

- No..... 0 *Skip to DM-9b*
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9 } *Skip to DM-9b*

DM-9a. At any of those times you were seen, were you offered an HIV test? An HIV test checks whether someone has the virus that causes AIDS.

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

Skip to DM-9c.

DM-9b. About how long has it been since you last saw a doctor, nurse, or other health care provider about your own health? Would you say it was...**[READ CHOICES. CHECK ONLY ONE.]**

- Within the past 5 years..... 1
- More than 5 years ago..... 2
- Refused to answer..... 7
- Don't know..... 9

DM-9c. During the past 12 months, was there any time when you needed medical care but didn't get it because you couldn't afford it?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

DM-10. Do you consider yourself to be: **[READ CHOICES. CHECK ONLY ONE.]**

- Heterosexual or "Straight"..... 1
- Homosexual, Gay, or Lesbian..... 2
- Bisexual..... 3
- Refused to answer..... 7
- Don't know..... 9

If DM-10 in (1, 7, 9), skip to DM-11.

If Respondent is male (ES9=1), ask DM-10a. Otherwise, skip to Say Box before DM-11.

DM-10a. Have you ever told anyone that you are attracted to or have sex with men?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

If DM-10a in (0, 7, 9), skip to DM-11.

DM-10b. I'm going to read you a list of people you may have told. Please tell me which ones apply. Have you told: **[READ CHOICES, CHECK NO OR YES FOR EACH ONE.]**

- | | No | Yes | Refused to answer | Does not Apply | Don't know |
|---|-------------------------------|---------------------------------|--------------------------------|--------------------------------|----------------------------|
| 1. Gay, lesbian, or bisexual friends | <input type="checkbox"/> 0... | <input type="checkbox"/> 1..... | <input type="checkbox"/> 7.... | <input type="checkbox"/> 8.... | <input type="checkbox"/> 9 |
| 2. Friends who are not gay, lesbian, or bisexual..... | <input type="checkbox"/> 0... | <input type="checkbox"/> 1..... | <input type="checkbox"/> 7.... | <input type="checkbox"/> 8.... | <input type="checkbox"/> 9 |
| 3. Family members..... | <input type="checkbox"/> 0... | <input type="checkbox"/> 1..... | <input type="checkbox"/> 7.... | <input type="checkbox"/> 8.... | <input type="checkbox"/> 9 |

FOR NHBS-IDU AND NHBS-HET: ASK DM-10b.4

- | | | | | | |
|------------------------------|-------------------------------|---------------------------------|--------------------------------|--------------------------------|----------------------------|
| 4. Spouse or partner..... | <input type="checkbox"/> 0... | <input type="checkbox"/> 1..... | <input type="checkbox"/> 7.... | <input type="checkbox"/> 8.... | <input type="checkbox"/> 9 |
| 5. Health care provider..... | <input type="checkbox"/> 0... | <input type="checkbox"/> 1..... | <input type="checkbox"/> 7.... | <input type="checkbox"/> 8.... | <input type="checkbox"/> 9 |

DM-11. During the past 12 months, have any of the following things happened to you because someone knew or assumed you were attracted to men? **[READ CHOICES, CHECK NO OR YES FOR EACH ONE.]**

	No	Yes	Refused to answer	Does not apply	Don't know
a. You were called names or insulted	0	1	7		9
b. You received poorer services than other people in restaurants, stores, other businesses or agencies	0	1	7		9
c. You were treated unfairly at work or school	0	1	7	8	9
d. You were denied or given lower quality health care	0	1	7	8	9
e. You were physically attacked or injured	0	1	7		9

DM-12. Next, I'm going to read you a statement. Please tell me how strongly you agree or disagree with it, using one of the options on this card. **[Give participant Flashcard G.]**
Most people in [project area] are tolerant of gays and bisexuals. Do you...[Read choices. Mark only one.]

- | | |
|---------------------------------|-----------------------------|
| Strongly agree..... | <input type="checkbox"/> 01 |
| Agree..... | <input type="checkbox"/> 02 |
| Neither agree nor disagree..... | <input type="checkbox"/> 03 |
| Disagree..... | <input type="checkbox"/> 04 |
| Strongly disagree..... | <input type="checkbox"/> 05 |
| Refused to answer..... | <input type="checkbox"/> 07 |
| Don't know..... | <input type="checkbox"/> 09 |

SEXUAL BEHAVIOR (SX)

SAY: Next, I'm going to ask you some questions about having sex. Please remember your answers will be kept private. **GIVE RESPONDENT FLASHCARD H.1**

For these questions, "having sex" means oral, vaginal, or anal sex. Oral sex means mouth on the vagina or penis; vaginal sex means penis in the vagina; and anal sex means penis in the anus (butt). I need to ask you all the questions, even if some may not apply to your situation.

Interviewer: Use your discretion in using slang terms for the following sexual behavior questions.

INTERVIEWER INSTRUCTIONS: Refer to response to Gender Question (ES9).

Male



**For NHBS-MSM, go to logic check before SX-2
FOR NHBS-IDU, GO TO SX-1
FOR NHBS-HET, GO TO SX-2.**

Female



**FOR NHBS-IDU, GO TO SX-54
FOR NHBS-HET, GO TO SX-55**

Transgender or Gender unknown



**FOR ALL CYCLES, GO TO SAY BOX
BEFORE AL-1**

FOR MALE RESPONDENTS ONLY

Female Sex Partners (Male respondent)

SX-1. Have you ever had vaginal or anal sex with a woman?

No..... 0

Yes..... 1

Refused to answer..... 7

Don't know..... 9

If SX-1 in (0, 7, 9), skip to SX-26.

If NHBS-MSM and ES9a in (0, 7, 9), skip to SAY Box before SX-26.

SX-2. How old were you the first time you had vaginal or anal sex with a woman?

[77 = Refused, 99 = Don't know] — —

SX-3. In the past 12 months, that is, since <interview month> of last year, with how many different women have you had oral, vaginal, or anal sex?

[Refused = 7777, Don't know = 9999] _____

NHBS-MSM & NHBS-IDU Skip Pattern for # of Female Sex Partners:

If SX-3 =1: Ask SX-4a. (RT column)
If SX-3 > 1: Ask SX-4. (LT column)
If SX-3 = 0, 7777, or 9999: Go to SAY Box before SX-26

NHBS-HET Skip Pattern for # of Female Sex Partners:

If SX-3 =1: Ask SX-4a. (RT column)
If SX-3 > 1: Ask SX-4. (LT column)
If SX-3 = 0, 7777, or 9999: Go to CONF13.

CONF-13. Sex partner confirmation (NHBS-HET):

If SX-3=0, 7777, or 9999, read:

I would like to clarify your response. You indicated that you haven't had sex with a woman in the past 12 months. Is that correct?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

If NO (NOT correct), go to SX-3 (ask it again)

If YES, (correct), Refused, or Don't know, go to END of Questionnaire.

FOR MULTIPLE FEMALE SEX PARTNERS [Read Say Box and Questions in this column]			FOR ONE FEMALE SEX PARTNER [Read Say Box and Question in this column]
<p>SAY: Now I'm going to ask you to describe these sex partners as either main or casual partners. [GIVE RESPONDENT FLASHCARD I]</p> <p>By “main partner” I mean a woman you have sex with and who you feel committed to above anyone else. This is a partner you would call your girlfriend, wife, significant other, or life partner. And by “casual partner” I mean a woman you have sex with but do not feel committed to or don't know very well. Refused = 7777, Don't know = 9999</p>			<p>SAY: Now I'm going to ask you to describe this sex partner as either a main or casual, partner. [GIVE RESPONDENT FLASHCARD I]</p> <p>By “main partner” I mean a woman you have sex with and who you feel committed to above anyone else. This is a partner you would call your girlfriend, wife, significant other, or life partner. And by “casual partner” I mean a woman you have sex with but do not feel committed to or don't know very well.</p>
<i>Question</i>	<i>Response</i>	<i>Skip Pattern</i>	<i>Question</i>
<p>SX-4. Of the _____ <i>[insert number from SX-3]</i> women you've had oral, vaginal, or anal sex with in the past 12 months, how many of them were main partners?</p>	[_____]	<i>If SX-4= SX-3, skip to Say Box before SX-6a.</i>	<p>SX 4a. Was this woman a main partner or a casual partner?</p> <p>Main partner..... <input type="checkbox"/> 1 <i>Skip to Say Box before SX-6a</i></p> <p>Casual partner..... <input type="checkbox"/> 2 <i>Skip to Say Box before SX-7a</i></p> <p>Refused to answer.. <input type="checkbox"/> 7</p> <p>Don't know..... <input type="checkbox"/> 9</p> <p>} <i>Skip to SX-8</i></p>
<p>SX-5. How many were casual partners?</p>	[_____]		

Skip Pattern for Multiple Female Sex Partners:
If SX-4 ≠ 0, 7777, or 9999: Go to Say Box before SX-6a.
Otherwise, if SX-5 ≠ 0, 7777, or 9999: Go to Say Box before SX-7a.

MAIN PARTNERS

MULTIPLE MAIN FEMALE PARTNERS [Read questions in this column] Refused = 7777, Don't know = 9999			ONE MAIN FEMALE PARTNER [Read questions in this column] No = 0, Yes = 1, Refused = 7, Don't know = 9		
SAY: Now I'm going to ask you about the _____ [insert number from SX-4] female main sex partners you had in the past 12 months.			SAY: Now I'm going to ask you about the female main sex partner you had in the past 12 months.		
<i>Question</i>	<i>Response</i>	<i>Skip Pattern</i>	<i>Question</i>	<i>Response</i>	<i>Skip Pattern</i>
SX-6a. Of your _____ [insert number from SX-4] female main partners in the past 12 months, with how many did you have vaginal sex?	[_____]	If 0, 7777, or 9999, skip to SX-6c.	SX-6a. In the past 12 months, did you have vaginal sex with this woman?	[_____]	If 0, 7, or 9, skip to SX-6c.
SX-6b. In the past 12 months, with how many of these _____ [insert number from SX-6a] women did you have vaginal sex without using a condom?	[_____]		SX-6b. In the past 12 months, did you have vaginal sex with her without using a condom?	[_____]	
SX-6c. Of your _____ [insert number from SX-4] female main partners in the past 12 months, with how many did you have anal sex?	[_____]	If 0, 7777, or 9999, skip to SX-6e.	SX-6c. In the past 12 months, did you have anal sex with this woman?	[_____]	If 0, 7, or 9, skip to SX-6e.
SX-6d. In the past 12 months, with how many of these _____ [insert number from SX-6c] women did you have anal sex without using a condom?	[_____]		SX 6d. In the past 12 months, did you have anal sex with her without using a condom?	[_____]	
SX6e. Of your _____ [insert number from SX-44] female main partners, how many did you have sex with for the very first time in the past 12 months?	[_____]		SX-6e. Think about the very first time you had sex with this woman. Was it within the past 12 months?	[_____]	
SX-6f. Of your _____ [insert number from SX-4] female main partners in the past 12 months, how many did you give things like money or drugs in exchange for sex?			SX-6f. In the past 12 months, did you give this woman things like money or drugs in exchange for sex?		
SX-6g. Of your _____ [insert number from SX-4] female main partners in the past 12 months, how many gave you things like money or drugs in exchange for sex?			SX-6g. In the past 12 months, did this woman give you things like money or drugs in exchange for sex?		If SX-4a=1, skip to SX-9.

Skip Pattern for Multiple Female Sex Partners:

If SX-4 = SX-3:

Skip to SX-9.

Otherwise, if SX-5 ≠ 0, 7777, or 9999:

Go to Say Box before SX-7a.

CASUAL PARTNERS

MULTIPLE CASUAL FEMALE PARTNERS [Read questions in this column] Refused = 7777, Don't know = 9999			ONE CASUAL FEMALE PARTNER [Read questions in this column] No = 0, Yes = 1, Refused = 7, Don't know = 9		
SAY: Now I'm going to ask you about the _____ [insert number from SX-5] female casual sex partners you had in the past 12 months. Remember, a casual sex partner is someone you do not feel committed to or don't know very well.			SAY: Now I'm going to ask you about the female casual sex partner you had in the past 12 months. Remember, a casual sex partner is someone you do not feel committed to or don't know very well.		
<i>Question</i>	<i>Response</i>	<i>Skip Pattern</i>	<i>Question</i>	<i>Response</i>	<i>Skip Pattern</i>
SX-7a. Of your _____ [insert number from SX-5] female casual partners in the past 12 months, with how many did you have vaginal sex?	[_____]	If 0, 7777, or 9999, skip to SX-7c.	SX-7a. In the past 12 months, did you have vaginal sex with this woman?	[_____]	If 0, 7, or 9, skip to SX-7c
SX-7b. In the past 12 months, with how many of these _____ [insert number from SX-7a] women did you have vaginal sex without using a condom?	[_____]	If 0, 7777, or 9999, skip to SX-7c.	SX-7b. In the past 12 months, did you have vaginal sex with her without using a condom?	[_____]	If 0, 7777, or 9999, skip to SX-7c.
SX-7c. Of your _____ [insert number from SX-5] female casual partners in the past 12 months, with how many did you have anal sex?	[_____]	If 0, 7777, or 9999, skip to SX-7e.	SX-7c. In the past 12 months, did you have anal sex with this woman?	[_____]	If 0, 7, or 9, skip to SX-7e.
SX-7d. In the past 12 months, with how many of these _____ [insert number from SX-7c] women did you have anal sex without using a condom?	[_____]		SX-7d. In the past 12 months did you have anal sex with her without using a condom?	[_____]	
SX-7e. Of your _____ [insert number from SX-4] female casual partners, how many did you have sex with for the very first time in the past 12 months?	[_____]		SX-7e. Think about the very first time you had sex with this woman. Was it within the past 12 months?	[_____]	
SX-7f. Of your _____ [insert number from SX-5] female casual partners in the past 12 months, how many did you give things like money or drugs in exchange for sex?			SX-7f. In the past 12 months, did you give this woman things like money or drugs in exchange for sex?		
SX-7g. Of your _____ [insert number from SX-5] female casual partners in the past 12 months, how many gave you things like money or drugs in exchange for sex?			SX-7g. In the past 12 months, did this woman give you things like money or drugs in exchange for sex?		If SX-4a=2, skip to SX-9.

If SX-3=1 and SX4a ≠ 7 OR 9, skip to SX-9.

SX-8. In the past **12 months**, did you have anal or vaginal sex without a condom with a woman whose HIV status you didn't know?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

SX-8a . In the past **12 months** did you have vaginal or anal sex without a condom with a woman who was HIV negative?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

SX-8b . In the past **12 months**, did you have vaginal or anal sex without a condom with a woman who was HIV positive?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

SX-9. Now I would like you to think about the last time you had sex with a woman. When was the last time you had oral, vaginal, or anal sex with a woman? Just tell me the month and year.

[77/7777 = Refused, 99/9999 = Don't know]

(M M / Y Y Y Y)

If SX-9 = 77/7777 or 99/9999, go to CONF14.

CONF14. INTERVIEWER, ask:

Did you have sex with a man in the past 12 months, that is, since &[AGO_1Y]?

- No..... 0**
- Yes..... 1**
- Don't know..... 9**
- Refuse to answer..... 7**

SX-12. When you had sex that last time, did you have vaginal sex?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

SX13. During vaginal sex that last time, did you or your partner use a condom?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

SX-13a. Did you or your partner use the condom the whole time?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

SX-14. Did you or your partner use the condom to prevent pregnancy, to prevent infections like HIV or other sexually transmitted diseases, to prevent both, or for some other reason?

- Pregnancy 1
- HIV/STDs..... 2
- Both..... 3
- Other reason..... 4
- Refused to answer..... 7
- Don't know..... 9

If participant did not report anal sex with only female partner or did not report anal sex with any female partners of the type identified for last female partner, skip to SX-17.

SX-15. When you had sex that last time, did you have anal sex?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

If SX-15 in (0, 7, 9), skip to CONF15.

- SX-16. During anal sex that last time, did you use a condom?
- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

If SX-16 in (0, 7, 9), skip to SX-17.

- SX-16a. Did you use the condom the whole time?
- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

CONF-15 Confirmation Message: Ask the following if SX-12 and SX-15 = 0:

"So this means you only had oral sex the last time you had sex?"
If participant says "No," go back to SX-12.

- SX-17. Before or during the last time you had sex with this partner, did you use:
[READ CHOICES. CHECK only ONE.]
- Alcohol..... 1
- Drugs..... 2
- Both alcohol and drugs..... 3
- Neither one..... 4
- Refused to answer..... 7
- Don't know..... 9

If SX-17 in (1, 4, 7, 9), skip to SX-18.

SX-17a. Which drugs did you use? **[DO NOT read choices. CHECK ALL that apply.]**

- Marijuana 1
- Speedballs (heroin and cocaine together) 2
- Heroin 3
- Crack cocaine..... 4
- Powdered cocaine 5
- Crystal meth (tina, crank, ice) 6
- X or Ecstasy 7
- Special K (ketamine) 8
- GHB 9
- Painkillers (Oxycontin, Vicodin, Percocet) 10
- Downers (Valium, Ativan, Xanax) 11
- Hallucinogens (LSD, mushrooms) 12
- Poppers 13
- Other drug 14
- Refused to answer..... 77
- Don't know..... 99

SX-18. The last time you had sex with this partner, did you know her HIV status?

- No..... 0 **Skip to SX-19**
- Yes..... 1
- Refused to answer..... 7 **Skip to SX-19**

SX-18a. What was her HIV status?

- HIV-negative..... 1
- HIV-positive..... 2
- Indeterminate..... 3
- Refused to answer..... 7

SX-19. Was this partner younger than you, older than you, or the same age as you?

- Younger 0
- Older 1
- Same age 2
- Refused to answer..... 7
- Don't know..... 9

If SX-19 in (0, 2, 7, 9), skip to SX-20.

SX-19a. What was her age? _____ [777 = Refused, 999 = Don't know]

SX-19b. Which of the following best describes her racial or ethnic background? **[READ choices. Choose one.]**

- American Indian or Alaska Native..... 1
- Asian 2
- Black or African American 3
- Hispanic or Latino..... 4
- Native Hawaiian or Other Pacific Islander..... 5
- White..... 6
- Refused to answer..... 7
- Don't know..... 9

SX-20. As far as you know, has this partner ever injected drugs like heroin, cocaine, or speed?
Would you say she: **[READ CHOICES. Check only ONE.]**

- Definitely did not..... 0
- Probably did not..... 1
- Probably did..... 2
- Definitely did 3
- Refused to answer..... 7
- Don't know..... 9

SX-21. As far as you know, has this partner ever used crack cocaine?
Would you say she: **[READ CHOICES. Check only ONE.]**

- Definitely did not..... 0
- Probably did not..... 1
- Probably did..... 2
- Definitely did 3
- Refused to answer..... 7
- Don't know..... 9

SX-22. As far as you know, has this partner ever been in prison or jail for more than 24 hours?
Would you say she: **[READ CHOICES. Check only ONE.]**

- Definitely did not..... 0
- Probably did not..... 1
- Probably did..... 2
- Definitely did 3
- Refused to answer..... 7
- Don't know..... 9

SX-23. How long have you been having a sexual relationship with this partner? (Please tell me how many days, months, or years). **[Interviewer: If "one night stand," enter 0]**

of Days: ___ ___

of Months: ___ ___

of Years: ___ ___

[Refused = 777, Don't know = 999]

If SX-23 > 12 months, skip to SX-25
If SX-23=0, skip to Say box before SX-26.

SX-24. As far as you know, during the time you were having a sexual relationship with this partner, did she have sex with other people? Would you say she: **[READ CHOICES. Check only ONE.]**

- Definitely did not..... 0
- Probably did not..... 1
- Probably did..... 2
- Definitely did 3
- Refused to answer..... 7
- Don't know..... 9

SX-24a. During the time you were having a sexual relationship with this partner, did you have sex with other people?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

If SX-23 ≤ 12 months, skip to SX-26

SX-25. As far as you know, during the past 12 months when you were having a sexual relationship with this partner, did she have sex with other people? Would you say she: **[READ CHOICES. Check only ONE.]**

- Definitely did not..... 0
- Probably did not..... 1
- Probably did..... 2
- Definitely did 3
- Refused to answer..... 7
- Don't know..... 9

SX-25a. During the past 12 months when you were having a sexual relationship with this partner, did you have sex with other people?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

Male Sex Partners (Male respondent)

SAY: Now I'm going to ask you some questions about having sex with other men. I need to ask you these questions even if some don't apply to you. Please remember your answers will be kept private.
[GIVE RESPONDENT FLASHCARD H.2]

For these questions, "having sex" means oral or anal sex. Oral sex means he put his mouth on your penis or you put your mouth on his penis. Anal sex means you put your penis in his anus (butt) or he put his penis in your anus (butt).

If NHBS-MSM, skip to SX-27.

- SX-26. Have you ever had oral or anal sex with a man?
- | | | | |
|------------------------|--------------------------|---|--------------------------------------|
| No..... | <input type="checkbox"/> | 0 | } <i>Skip to Say Box before AL-1</i> |
| Yes..... | <input type="checkbox"/> | 1 | |
| Refused to answer..... | <input type="checkbox"/> | 7 | |
| Don't know..... | <input type="checkbox"/> | 9 | |

SX-27. How old were you the first time you had oral or anal sex with a man?

[77 = Refused, 99 = Don't know] _ _

SX-28. In the past 12 months, that is, since *<interview month>* of last year, with how many different men have you had oral or anal sex?

[Refused = 7777, Don't know = 9999] _ _ _ _

**If SX-28 ≥ 1 and SX-28 < 7777, skip to SX-29.
 If SX-28 = 0, ask SX-28a, then skip to SX-50.**

SX-28a. Think about the last time you had either oral or anal sex with a man. How many years ago was that?

[Refused = 7777, Don't know = 9999] _ _ _ _ *Range: 1–99*

**Skip Pattern for # of Male Sexual Partners: If SX-28 =1, ask SX-29a.
 Otherwise, ask SX-29.**

FOR MULTIPLE MALE PARTNERS [Read Say Box and Questions in this column]			FOR ONE MALE PARTNER [Read Say Box and Question in this column]
<p>SAY: Now I'm going to ask you to describe these sex partners as either main or casual partners. [GIVE RESPONDENT FLASHCARD J]</p> <p>By “main partner” I mean a man you have sex with and who you feel committed to above anyone else. This is a partner you would call your boyfriend, husband, significant other, or life partner. And by “casual partner” I mean a man you have sex with but do not feel committed to or don't know very well.</p> <p>Refused = 7777, Don't know = 9999</p>			<p>SAY: Now I'm going to ask you to describe this sex partner as either main or casual partners. [GIVE RESPONDENT FLASHCARD J]</p> <p>By “main partner” I mean a man you have sex with and who you feel committed to above anyone else. This is a partner you would call your boyfriend, husband, significant other, or life partner. And by “casual partner” I mean a man you have sex with but do not feel committed to or don't know very well.</p>
<i>Question</i>	<i>Response</i>	<i>Skip Pattern</i>	<i>Question</i>
SX-29. Of the _____ [insert number from SX-28] men you've had oral or anal sex with in the past 12 months, how many of them were main partners?	[_____]	<i>If SX-29 = SX-28, skip to Say Box before SX-31a.</i>	SX-29a. Was this man a main partner or a casual partner?
SX-30. How many were casual partners?	[_____]		Main partner..... <input type="checkbox"/> 1 → <i>Skip to SX-31a</i> Casual partner..... <input type="checkbox"/> 2 → <i>Skip to SX-32a</i> Refused to answer.... <input type="checkbox"/> 7 } Don't know..... <input type="checkbox"/> 9 } <i>Skip to SX-33</i>
<p>Skip Pattern For Multiple Male Partners: <i>If SX-29 is not equal to 0, 7777, or 9999, go to Say Box before SX31a.</i> <i>Otherwise, if SX-30 is not equal to 0, 7777, or 9999, go to Say Box before SX-32a.</i></p>			

MAIN MALE PARTNERS

MULTIPLE MAIN MALE PARTNERS [Read questions in this column] Refused = 7777, Don't know = 9999			ONE MAIN MALE PARTNER [Read questions in this column] No = 0, Yes = 1, Refused = 7, Don't know = 9		
SAY: Now I'm going to ask you about the _____ [insert number from SX-29] male main sex partners you had in the past 12 months.			SAY: Now I'm going to ask you about the male main sex partner you had in the past 12 months.		
<i>Question</i>	<i>Response</i>	<i>Skip Pattern</i>	<i>Question</i>	<i>Response</i>	<i>Skip Pattern</i>
SX-31a. Of your _____ [insert number from SX-29] male main partners in the past 12 months, with how many did you have anal sex?	[_____]	<i>If 0, 7777, or 9999, skip to SX-31c.</i>	SX-31a. In the past 12 months, did you have anal sex with this man?	[_____]	<i>If 0, 7, or 9, skip to SX-31c.</i>
SX-31b. In the past 12 months, with how many of these _____ [insert number from SX-31a] men did you have anal sex without using a condom?	[_____]		SX-31b. In the past 12 months, did you have anal sex with him without using a condom?	[_____]	
SX-31b.1. Did you know the HIV status of any of these _____ [insert number from SX-31b] men?	0 = no 1 = yes 7 = Ref	<i>If 0 or 7, skip to SX-31c.1</i>	SX-31b.1. Did you know his HIV status?	0 = no 1 = yes 7 = Ref	<i>If 0 or 7, skip to SX-31c.1</i>
SX-31b.2. For how many of these men did you know their HIV status?	[_____]	<i>If 1, ask single partner version of SX-31b.2, then go to SX-31c.</i>	SX-31b.2. What was his HIV status?	HIV-positive...1 HIV-negative...2 Indeterminate...3 Refused.....7	
SX-31b.3. Of those _____ [insert number from SX-31b.2] men, how many did you know were HIV-positive?	[_____]				
SX-31b.4. How many did you know were HIV-negative?	[_____]				
Soft edit check					
SX-31c. Of your _____ [insert number from SX-29] male main partners, how many did you have sex with for the very first time in the past 12 months?	[_____]		SX-31c. Think about the very first time you had sex with this man. Was it within the past 12 months?	[_____]	
SX-31d. Of your _____ [insert number from SX-29] male main partners in the past 12 months, how many did you give things like money or drugs in exchange for sex?			SX-31d. In the past 12 months, did you give this man things like money or drugs in exchange for sex?		

MULTIPLE MAIN MALE PARTNERS [Read questions in this column] Refused = 7777, Don't know = 9999		ONE MAIN MALE PARTNER [Read questions in this column] No = 0, Yes = 1, Refused = 7, Don't know = 9	
SX-31e. Of your _____ <i>[insert number from SX-29]</i> male main partners in the past 12 months, how many <u>gave</u> <u>you things</u> like money or drugs in exchange for sex?		SX-31e. In the past 12 months, did this man <u>give</u> <u>you</u> things like money or drugs, in exchange for sex?	<i>If SX-29a=1, skip to QSX- 33.</i>

Skip Pattern for Multiple Male Sex Partners:
If SX-29= SX-28, Skip to SX-33.
Otherwise, if SX-30 is not equal to 0, 7777, or 9999, go to Say Box before SX-32a.

CASUAL PARTNERS

MULTIPLE CASUAL MALE PARTNERS [Read questions in this column] Refused = 7777, Don't know = 9999			ONE CASUAL MALE PARTNER [Read questions in this column] No = 0, Yes = 1, Refused = 7, Don't know = 9		
<p>SAY: Now I'm going to ask you about the _____ <i>[insert number from SX-30]</i> male casual sex partners you had in the past 12 months. Remember, a casual sex partner is someone you do not feel committed to or don't know very well.</p>			<p>SAY: Now I'm going to ask you about the male casual sex partner you had in the past 12 months. Remember, a casual sex partner is someone you do not feel committed to or don't know very well.</p>		
<i>Question</i>	<i>Response</i>	<i>Skip Pattern</i>	<i>Question</i>	<i>Response</i>	<i>Skip Pattern</i>
SX-32a. Of your _____ <i>[insert number from SX-30]</i> male casual partners in the past 12 months, with how many did you have anal sex?	[_____]	<i>If 0, 7777, or 9999, skip to SX-32c.</i>	SX-32a. In the past 12 months, did you have anal sex with this man?	[_____]	<i>If 0, 7, or 9, skip to SX-32c.</i>
SX-32b. In the past 12 months, with how many of these _____ <i>[insert number from SX-32a]</i> men did you have anal sex without using a condom?	[_____]		SX-32b. In the past 12 months, did you have anal sex without using a condom?	[_____]	
SX-32b.1. Did you know the HIV status of any of these _____ <i>[insert number from SX-32b]</i> men?	0 = no 1 = yes 7 = Ref	<i>If 0 or 7, skip to SX-32c.</i>	SX-32b.1. Did you know his HIV status?	0 = no 1 = yes 7 = Ref	<i>If 0 or 7, skip to SX-32c.</i>
SX-32b.2. For how many of these men did you know their HIV status?	[_____]	<i>If 1, ask single partner version of SX-32b.2, then go to SX-32c.</i>	SX-32b.2. What was his HIV status?	HIV-positive...1 HIV-negative...2 Indeterminate...3 Refused.....7	
SX-32b.3. Of those _____ <i>[insert number from SX-32b.2]</i> men, how many did you know were HIV-positive?	[_____]				
SX-32b.4. How many did you know were HIV-negative?	[_____]				
Soft edit check					
SX-32c. Of your _____ <i>[insert number from SX-30]</i> male casual partners, how many did you have sex with <u>for the very first time</u> in the past 12 months?	[_____]		SX-32c. Think about the very first time you had sex with this man. Was it within the past 12 months?	[_____]	

MULTIPLE CASUAL MALE PARTNERS [Read questions in this column] Refused = 7777, Don't know = 9999			ONE CASUAL MALE PARTNER [Read questions in this column] No = 0, Yes = 1, Refused = 7, Don't know = 9		
SX-32d. Of your _____ <i>[insert number from SX-30]</i> male casual partners in the past 12 months, how many <u>did you give</u> things like money or drugs in exchange for sex?			SX-32d. In the past 12 months, did <u>you give</u> this man things like money or drugs in exchange for sex?		
SX-32e. Of your _____ <i>[insert number from SX-30]</i> male casual partners in the past 12 months, how many <u>gave you things</u> like money or drugs in exchange for sex?			SX-32e. In the past 12 months, did this man <u>give you things</u> like money or drugs, in exchange for sex?		

SX-33. Now I would like you to think about the last time you had sex with a man. When was the last time you had anal or oral sex with a man? Just tell me the month and year.

[77/7777 = Refused, 99/9999 = Don't know] (M M / Y Y / Y Y) --

If SX-33 = 77/7777 or 99/9999, go to CONF16.

CONF16. INTERVIEWER:
Did you have sex with a man in the past 12 months, that is, since &[AGO_1Y]?
No..... 0
Yes..... 1
Don't know..... 9
Refuse to answer..... 7

Skip Pattern:
If SX-28=1, go to SX-35.
Otherwise, if SX-28>1, ask SX-34.

SX-34. Was the man you had sex with that last time a main partner or a casual partner? **GIVE RESPONDENT FLASHCARD I.** Remember, a main sex partner is someone you feel committed to above anyone else. And a casual sex partner is someone you do not feel committed to or don't know very well.

- Main sex partner..... 1
- Casual sex partner..... 2
- Refused to answer..... 7
- Don't know..... 9

If participant had one male partner and reported NO exchange with only male partner, skip to SX-36.
If last male partner = main (SX-34 = 1) AND participant reported NO exchange with ANY male main partners, skip to SX-36.
If last male partner = casual (SX-34 = 2) and participant reported NO exchange with ANY male casual partners, skip to SX-36.

SX-35. When you had sex that last time, did you give him things like money or drugs in exchange for sex?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

SX-35a. When you had sex that last time, did he give you things like money or drugs in exchange for sex?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

SX-36. When you had sex that last time, did you have receptive anal sex where he put his penis in your anus (butt)?

- No..... 0 → *Skip to SX-38*
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9 } *Skip to SX-38*

SX-37. During receptive anal sex that last time, did he use a condom?

- No..... 0 → *Skip to SX-38*
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9 } *Skip to SX-38*

SX-37a. Did he use the condom the whole time?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

SX-38. When you had sex that last time, did you have insertive anal sex where you put your penis in his anus (butt)?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

If SX-38 in (0, 7, 9), skip to CONF17.

- SX-39. During insertive anal sex that last time, did you use a condom?
- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

If SX-39 in (0, 7, 9), skip to SX-40.

- SX-39a. Did you use the condom the whole time?
- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

**CONF17: Ask the following if SX-36 and SX-38 =0:
"So this means you only had oral sex the last time you had sex?"**

- SX-40. Before or during the last time you had sex with this partner, did you use:
[READ CHOICES. CHECK only ONE.]
- Alcohol..... 1
- Drugs..... 2
- Both alcohol and drugs..... 3
- Neither one..... 4
- Refused to answer..... 7
- Don't know..... 9

If SX-40 in (1, 4, 7, 9), skip to SX-41.

- SX-40a. Which drugs did you use? *[DO NOT read choices. Check ALL that apply.]*
- Marijuana 1
- Speedballs (heroin and cocaine together) 2
- Heroin 3
- Crack cocaine..... 4
- Powdered cocaine 5
- Crystal meth (tina, crank, ice) 6

- X or Ecstasy 7
- Special K (ketamine) 8
- GHB 9
- Painkillers (Oxycontin, Vicodin, Percocet) 10
- Downers (Valium, Ativan, Xanax) 11
- Hallucinogens (LSD, mushrooms) 12
- Poppers 13
- Other drug 14
- Refused to answer 77
- Don't know 99

If participant had one male sex partner in past 12 months, skip to SX-42.

SX-41. The last time you had sex with this partner, did you know his HIV status?

- No..... 0 ***Skip to SX-42***
- Yes..... 1
- Refused to answer..... 7 ***Skip to SX-42***

SX-41a. What was his HIV status?

- HIV-negative..... 1
- HIV-positive..... 2
- Indeterminate..... 3
- Refused to answer..... 7

SX-42. Was this partner younger than you, older than you, or the same age as you?

- Younger 0
- Older 1
- Same age 2
- Refused to answer..... 7
- Don't know..... 9

If SX-42 in (0, 2, 7, 9), skip to SX-43.

SX-42a. What was his age? _____ [777 = Refused, 999 = Don't know]

SX-42b. Which of the following best describes his racial or ethnic background? **[READ choices. Choose one.]**

- American Indian or Alaska Native..... 1
- Asian 2
- Black or African American 3
- Hispanic or Latino..... 4
- Native Hawaiian or Other Pacific Islander..... 5
- White..... 6
- Refused to answer..... 7
- Don't know..... 9

SX-43. As far as you know, has this partner ever injected drugs like heroin, cocaine, or speed? Would you say he: **[READ CHOICES. Check only ONE.]**

- Definitely did not..... 0
- Probably did not..... 1
- Probably did..... 2
- Definitely did 3
- Refused to answer..... 7
- Don't know..... 9

SX-44. As far as you know, has this partner ever used crack cocaine? Would you say he: **[READ CHOICES. Check only ONE.]**

- Definitely did not..... 0
- Probably did not..... 1
- Probably did..... 2
- Definitely did 3
- Refused to answer..... 7
- Don't know..... 9

SX-44a. As far as you know, has this partner ever used crystal meth (tina, crank, ice)?
Would you say he: **[READ CHOICES. Check only ONE.]**

- Definitely did not..... 0
- Probably did not..... 1
- Probably did..... 2
- Definitely did 3
- Refused to answer..... 7
- Don't know..... 9

SX-45. As far as you know, has this partner ever been in prison or jail for more than 24 hours?
Would you say he: **[READ CHOICES. Check only ONE.]**

- Definitely did not..... 0
- Probably did not..... 1
- Probably did..... 2
- Definitely did 3
- Refused to answer..... 7
- Don't know..... 9

SX-46. How long have you been having a sexual relationship with this partner? (Please tell me how many days, months, or years). **[Interviewer: If "one night stand," enter 0.]**

of Days: ___ ___

of Months: ___ ___

of Years: ___ ___

[Refused = 777, Don't know = 999]

If SX-46 > 12 months, 777, or 999, skip to SX-48. If SX-46=0, skip to SX-49.

SX-47. As far as you know, during the time you were having a sexual relationship with this partner, did he have sex with other people? Would you say he: **[READ CHOICES. Check only ONE.]**

- Definitely did not..... 0
- Probably did not..... 1
- Probably did..... 2
- Definitely did 3
- Refused to answer..... 7
- Don't know..... 9

- SX-47a. During the time you were having a sexual relationship with this partner, did you have sex with other people?
- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

If SX-46 ≤ 12 months, skip to SX-50.

- SX-48. As far as you know, during the past 12 months when you were having a sexual relationship with this partner, did he have sex with other people? Would you say he: ***[READ CHOICES. Check only ONE.]***
- Definitely did not..... 0
- Probably did not..... 1
- Probably did..... 2
- Definitely did 3
- Refused to answer..... 7
- Don't know..... 9

- SX-48a. During the past 12 months when you were having a sexual relationship with this partner, did you have sex with other people?
- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

If SX-46 > or = 3 years or SX-46 = Don't Know or Refused, skip to SX-50

- SX-49. Where did you first meet this partner? ***[DO NOT read choices. Check only ONE.]***
- Internet..... 01
- Chat line..... 02
- Bar/Club..... 03
- Circuit party or Rave..... 04
- Cruising area..... 05
- Adult bookstore..... 06
- Bath house, sex club or sex resort..... 07

- Private sex party..... 08
- Somewhere else..... 09
- Refused to answer..... 77
- Don't know..... 99

If NHBS-IDU OR NHBS-HET, skip to SX-52

SX-50. In the past 12 months, how often have you gone to a place where gay men hangout, meet or socialize? These could include bars, clubs, social organizations, parks, gay businesses, bookstores, sex clubs, etc. Was it: **[GIVE RESPONDENT FLASHCARD K. READ CHOICES. CHECK only ONE.]**

- | | | | | | | | | | |
|---------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|----------------------------------|-------------------------------|
| Never | More than once a day | Once a day | More than once a week | Once a week | More than once a month | Once a month | Less than once a month | Refused to answer | Don't Know |
| <input type="checkbox"/> 0..... | <input type="checkbox"/> 1..... | <input type="checkbox"/> 2..... | <input type="checkbox"/> 3..... | <input type="checkbox"/> 4..... | <input type="checkbox"/> 5..... | <input type="checkbox"/> 6..... | <input type="checkbox"/> 7..... | <input type="checkbox"/> 77..... | <input type="checkbox"/> ..99 |

SX-51. In the past 12 months, how often have you used the internet to meet or socialize with gay men either for *friendship or sex*? These could include social network websites (such as Facebook or MySpace), websites directed towards gay men (such as Manhunt or Gay.com), dating websites, or the use of mobile social applications (such as Foursquare or Grindr). Was it: **[GIVE RESPONDENT FLASHCARD K. READ CHOICES. CHECK only ONE.]**

- | | | | | | | | | | |
|---------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|----------------------------------|-------------------------------|
| Never | More than once a day | Once a day | More than once a week | Once a week | More than once a month | Once a month | Less than once a month | Refused to answer | Don't Know |
| <input type="checkbox"/> 0..... | <input type="checkbox"/> 1..... | <input type="checkbox"/> 2..... | <input type="checkbox"/> 3..... | <input type="checkbox"/> 4..... | <input type="checkbox"/> 5..... | <input type="checkbox"/> 6..... | <input type="checkbox"/> 7..... | <input type="checkbox"/> 77..... | <input type="checkbox"/> ..99 |

Skip Pattern: If DM-10 (Sexual identity)=1, ask SX-52. Otherwise, go to Say Box before AL-1.

SX-52. The next question is about whether you have told people that you are attracted to or have sex with men. Have you ever told anyone that you are attracted to or have sex with men?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

If SX-52 in (0, 7, 9), skip to SX-53.

SX-52a. I'm going to read you a list of people you may have told. Please tell me which ones apply. Have you told: **[READ CHOICES, CHECK NO OR YES FOR EACH ONE.]**

- | | No | Yes | Refused to answer | Does not Apply | Don't know |
|---|-------------------------------|---------------------------------|--------------------------------|--------------------------------|----------------------------|
| 1. Gay, lesbian, or bisexual friends | <input type="checkbox"/> 0... | <input type="checkbox"/> 1..... | <input type="checkbox"/> 7.... | <input type="checkbox"/> 8.... | <input type="checkbox"/> 9 |
| 2. Friends who are not gay, lesbian, or bisexual..... | <input type="checkbox"/> 0... | <input type="checkbox"/> 1..... | <input type="checkbox"/> 7.... | <input type="checkbox"/> 8.... | <input type="checkbox"/> 9 |
| 3. Family members..... | <input type="checkbox"/> 0... | <input type="checkbox"/> 1..... | <input type="checkbox"/> 7.... | <input type="checkbox"/> 8.... | <input type="checkbox"/> 9 |

FOR NHBS-IDU AND NHBS-HET: ASK SX-52a.4

- | | | | | | |
|------------------------------|-------------------------------|---------------------------------|--------------------------------|--------------------------------|----------------------------|
| 4. Spouse or partner..... | <input type="checkbox"/> 0... | <input type="checkbox"/> 1..... | <input type="checkbox"/> 7.... | <input type="checkbox"/> 8.... | <input type="checkbox"/> 9 |
| 5. Health care provider..... | <input type="checkbox"/> 0... | <input type="checkbox"/> 1..... | <input type="checkbox"/> 7.... | <input type="checkbox"/> 8.... | <input type="checkbox"/> 9 |

SX-53. During the past 12 months, have any of the following things happened to you because someone knew or assumed you were attracted to men? **[READ CHOICES, CHECK NO OR YES FOR EACH ONE.]**

	No	Yes	Refused to answer	Does not apply	Don't know
a. You were called names or insulted	0	1	7		9
b. You received poorer services than other people in restaurants, stores, other businesses or agencies	0	1	7		9
c. You were treated unfairly at work or school	0	1	7	8	9
d. You were denied or given lower quality health care	0	1	7	8	9
e. You were physically attacked or injured	0	1	7		9

SX-54. Next, I'm going to read you a statement. Please tell me how strongly you agree or disagree with it, using one of the options on this card. *[Give participant Flashcard G.]*

Most people in [project area] are tolerant of gays and bisexuals. Do you...[Read choices. Mark only one.]

- Strongly agree..... 01
- Agree..... 02
- Neither agree nor disagree..... 03
- Disagree..... 04
- Strongly disagree..... 05
- Refused to answer..... 07
- Don't know..... 09

END OF MALE RESPONDENT SECTION. GO TO SAY BOX BEFORE AL-1.

FOR FEMALE RESPONDENTS ONLY

Male Sex Partners (Female respondent)

- SX-54. Have you ever had vaginal or anal sex with a man?
- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

If SX-54 in (0, 7, 9), skip to SX-80.

- SX-55. How old were you the first time you had vaginal or anal sex with a man?
- [77 = Refused, 99 = Don't know]* _ _

- SX-56. In the past 12 months, that is, since *<interview month>* of last year, with how many different men have you had oral, vaginal, or anal sex?
- _____ *[Refused = 7777, Don't know = 9999]*

NHBS-IDU Skip Pattern for # of Male Sexual Partners:
If SX-56 =1, ask SX-57a.
If SX-56 >1, ask SX-57.
If 0, 7777, or 9999, skip to SX-80

NHBS-HET Skip Pattern for # of Female Sex Partners:
If SX-56 =1: Ask SX-57a. (RT column)
If SX-56 > 1: Ask SX-57. (LT column)
If SX-56 = 0, 7777, or 9999: Go to CONF18.

CONF18. Sex partner confirmation:

If SX-56=0, 7777, or 9999, read:
I would like to clarify your response. You indicated that you haven't had sex with a man in the past 12 months. Is that correct?

No..... 0

Yes..... 1

Refused to answer..... 7

Don't know..... 9

If NO (NOT correct), go to SX-56 (ask it again)
If YES, (correct), Refused to answer, or Don't know, go to End of Questionnaire.

FOR MULTIPLE MALE PARTNERS [Read Say Box and Questions in this column]			FOR ONE MALE PARTNER [Read Say Box and Question in this column]
<p>SAY: Now I'm going to ask you to describe the sex partners you've had in the past 12 months as either main or casual partners.</p> <p>[GIVE RESPONDENT FLASHCARD J]</p> <p>By “main partner” I mean a man you have sex with and who you feel committed to above anyone else. This is a partner you would call your boyfriend, husband, significant other, or life partner. And by “casual partner” I mean a man you have sex with but do not feel committed to or don't know very well.</p> <p>Refused = 7777, Don't know = 9999</p>			<p>SAY: Now I'm going to ask you to describe this sex partner you've had in the past 12 months as either a main or casual partner.</p> <p>[GIVE RESPONDENT FLASHCARD J]</p> <p>By “main partner” I mean a man you have sex with and who you feel committed to above anyone else. This is a partner you would call your boyfriend, husband, significant other, or life partner. And by “casual partner” I mean a man you have sex with but do not feel committed to or don't know very well.</p>
<i>Question</i>	<i>Response</i>	<i>Skip Pattern</i>	<i>Question</i>
SX-57. Of the ____ [<i>insert number from SX-56</i>] men you've had oral, vaginal, or anal sex with in the past 12 months, how many of them were main partners?	[_____]	<i>If SX-57= SX-56, skip to Say Box before SX-59a.</i>	SX-57a. Was this man a main partner or a casual partner? Main partner..... <input type="checkbox"/> 1 <i>Skip to Say Box before SX-59a</i> Casual partner..... <input type="checkbox"/> 2 <i>Skip to Say Box before SX-60a</i>
SX-58. How many were casual partners?	[_____]		Refused to answer... <input type="checkbox"/> 7 Don't know..... <input type="checkbox"/> 9 } <i>Skip to SX-61</i>

Skip Pattern for Multiple Male Partners:

If SX-57 is not equal to 0, 7777, or 9999, go to Say Box before SX-59a.

Otherwise, if SX-58 is not equal to 0, 7777, or 9999, go to Say Box before SX-60a.

MAIN MALE PARTNERS

<i>MULTIPLE MAIN MALE PARTNERS</i> [Read questions in this column] Refused = 7777, Don't know = 9999			<i>ONE MAIN MALE PARTNER</i> [Read questions in this column] No = 0, Yes = 1, Refused = 7, Don't know = 9		
SAY: Now I'm going to ask you about the _____ [<i>insert number from SX-57</i>] male main sex partners you had in the past 12 months.			SAY: Now I'm going to ask you about the male main sex partner you had in the past 12 months.		
<i>Question</i>	<i>Response</i>	<i>Skip Pattern</i>	<i>Question</i>	<i>Response</i>	<i>Skip Pattern</i>
SX-59a. Of your _____ [<i>insert number from SX-57</i>] male main partners in the past 12 months, with how many did you have vaginal sex?	[_____]	<i>If 0, 7777, or 9999, skip to SX-59c.</i>	SX-59a. In the past 12 months, did you have vaginal sex with this man?	[_____]	<i>If 0, 7, or 9, skip to SX-59c.</i>
SX-59b. In the past 12 months, with how many of these _____ [<i>insert number from SX-59a</i>] men did you have vaginal sex without using a condom?	[_____]		SX-59b. In the past 12 months, did you have vaginal sex with him without using a condom?	[_____]	
SX-59c. Of your _____ [<i>insert number from SX-57</i>] male main partners in the past 12 months, with how many did you have anal sex?	[_____]	<i>If 0, 7777, or 9999, skip to SX-59e.</i>	SX-59c. In the past 12 months, did you have anal sex with this man?	[_____]	<i>If 0, 7, or 9, skip to SX-59e.</i>
SX-59d. With how many of these _____ [<i>insert number from SX-59c</i>] men did you have anal sex without using a condom?	[_____]		SX-59d. In the past 12 months, did you have anal sex with him without using a condom?	[_____]	
SX-59e. Of your _____ [<i>insert number from SX-57</i>] male main partners, how many did you have sex with <u>for the very first time</u> in the past 12 months?	[_____]		SX-59e. Think about the very first time you had sex with this man. Was it within the past 12 months?	[_____]	
SX-59f. Of your _____ [<i>insert number from SX-57</i>] male main partners in the past 12 months, how many <u>gave you things</u> like money or drugs in exchange for sex?			SX-59f. In the past 12 months, did this man <u>give you</u> money, drugs, or other things in exchange for sex?		
SX-59g. Of your _____ [<i>insert number from SX-57</i>] male main partners in the past 12 months, how many <u>did you give</u> things like money or drugs in exchange for sex?			SX-59g. In the past 12 months, did <u>you give</u> this man things like money or drugs in exchange for sex?		<i>If SX-57a=1, skip to SX-62.</i>

Skip Pattern for Multiple Male Sex Partners:

If SX-57= SX-56, go to SX-62.

Otherwise, if SX-58 is not equal to 0, 7777, or 9999, go to Say Box before SX-60a .

CASUAL PARTNERS

MULTIPLE CASUAL MALE PARTNERS [Read questions in this column] Refused = 7777, Don't know = 9999			ONE CASUAL MALE PARTNER [Read questions in this column] No = 0, Yes = 1, Refused = 7, Don't know = 9		
SAY: Now I'm going to ask you about the _____ [<i>insert number from SX-58</i>] male casual sex partners you had in the past 12 months. Remember, a casual sex partner is someone you do not feel committed to or don't know very well.			SAY: Now I'm going to ask you about the male casual sex partner you had in the past 12 months. Remember, a casual sex partner is someone you do not feel committed to or don't know very well.		
<i>Question</i>	<i>Response</i>	<i>Skip Pattern</i>	<i>Question</i>	<i>Response</i>	<i>Skip Pattern</i>
SX-60a. Of your _____ [<i>insert number from SX-58</i>] male casual partners in the past 12 months, with how many did you have vaginal sex?	[_____]	<i>If 0, 7777, or 9999, skip to SX-60c.</i>	SX-60a. In the past 12 months, did you have vaginal sex with this man?	[_____]	<i>If 0, 7, or 9, skip to SX-60c.</i>
SX-60b. In the past 12 months, with how many of these _____ [<i>insert number from SX-60a</i>] men did you have vaginal sex without using a condom?	[_____]		SX-60b. In the past 12 months, did you have vaginal sex with him without using a condom?	[_____]	
SX-60c. Of your _____ [<i>insert number from SX-58</i>] male casual partners in the past 12 months, with how many did you have anal sex?	[_____]	<i>If 0, 7777, or 9999, skip to SX-60e.</i>	SX-60c. In the past 12 months, did you have anal sex with this man?	[_____]	<i>If 0, 7, or 9, skip to SX-60e.</i>
SX-60d. In the past 12 months, with how many of these _____ [<i>insert number from SX-60c</i>] men did you have anal sex without using a condom?	[_____]		SX-60d. In the past 12 months, did you have anal sex with him without using a condom?	[_____]	
SX-60e. Of your _____ [<i>insert number from SX-60</i>] male casual partners, how many did you have sex with <u>for the very first time</u> in the past 12 months?	[_____]		SX-60e. Think about the very first time you had sex with this man. Was it within the past 12 months?	[_____]	
SX-60f. Of your _____ [<i>insert number from SX-58</i>] male casual partners in the past 12 months, how many <u>gave you things</u> like money or drugs in exchange for sex?			SX-60f. In the past 12 months, did this man <u>give you</u> money, drugs, or other things in exchange for sex?		
SX-60g. Of your _____ [<i>insert number from SX-58</i>] male casual partners in the past 12 months, how many <u>did you give</u> things like money or drugs in exchange for sex?			SX-60g. In the past 12 months, did <u>you give</u> this man things like money or drugs in exchange for sex?		

If SX-56=1 AND SX-57a ≠ 7 OR 9, skip to SX-62.

SX-61. In the past **12 months**, did you have anal or vaginal sex without a condom with a man whose HIV status you didn't know?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

SX-61a. In the past **12 months** did you have vaginal or anal sex without a condom with a man who was HIV negative?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

SX-61b. In the past **12 months**, did you have vaginal or anal sex without a condom with a man who was HIV positive?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

SX-62. Now I would like you to think about the last time you had sex with a man. When was the last time you had oral, vaginal, or anal sex with a man? Just tell me the month and year.

[77/7777 = Refused, 99/9999 = Don't know] (M M / Y Y Y Y)

If SX-62 = 77/7777 OR 99/9999, go to CONF19.

CONF19. INTERVIEWER:

Did you have sex with a man in the past 12 months, that is, since &[AGO_1Y]?

- No..... 0
- Yes..... 1
- Don't know..... 9
- Refuse to answer..... 7

If SX-56=1, go to SX-64. Otherwise if SX-56>1, ask SX-63.

SX-63. Was the man you had sex with that last time a main partner or a casual partner? ***GIVE RESPONDENT FLASHCARD J.*** Remember, a main sex partner is someone you feel committed to above anyone else. And a casual sex partner is someone you do not feel committed to or don't know very well.

- Main sex partner..... 1
Casual sex partner..... 2
Refused to answer..... 7
Don't know..... 9

***If participant had 1 partner and reported NO exchange with only partner, skip to SX-65.
If participant's last partner was main partner and participant reported NO exchange with ANY main partners, skip to SX-65.
If participant's last partner was casual and participant reported NO exchange with ANY casual partners, skip to SX-65.***

SX-64. When you had sex that last time, did he give you things like money or drugs in exchange for sex?

- No..... 0
Yes..... 1
Refused to answer..... 7
Don't know..... 9

SX-64a. When you had sex that last time, did you give him things like money or drugs in exchange for sex?

- No..... 0
Yes..... 1
Refused to answer..... 7
Don't know..... 9

SX-65. When you had sex that last time, did you have vaginal sex?

- No..... 0 → *Skip to Logic check before SX-68*
Yes..... 1
Refused to answer..... 7 }
Don't know..... 9 } *Skip to Logic check before SX-68*

- SX-66. During vaginal sex that last time, did you or your partner use a condom?
- No..... 0 → *Skip to Logic check before SX-68*
- Yes..... 1
- Refused to answer..... 7 } *Skip to Logic check before SX-68*
- Don't know..... 9 }

- SX-66a. Did you or your partner use the condom the whole time?
- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

- SX-67. Did you or your partner use the condom to prevent pregnancy, to prevent infections like HIV or other sexually transmitted diseases, to prevent both, or for some other reason?
- Pregnancy 1
- HIV/STDs..... 2
- Both..... 3
- Other reason..... 4
- Refused to answer..... 7
- Don't know..... 9

If participant had 1 male partner and reported NO anal sex with that partner, skip to SX-70.
If participant's last partner was main and participant reported NO anal sex with ANY main partners, skip to SX-70.
If participant's last partner was casual and participant reported NO anal sex with ANY casual partners, skip to SX-70.

- SX-68. When you had sex that last time, did you have anal sex?
- No..... 0 → *Skip to CONF20.*
- Yes..... 1
- Refused to answer..... 7 } *Skip to CONF20.*
- Don't know..... 9 }

- SX-69. During anal sex that last time, did your partner use a condom?
- No..... 0 → *Skip to SX-70*
- Yes..... 1
- Refused to answer..... 7 } *Skip to SX-70*
- Don't know..... 9 }

- SX-69a. Did he use the condom the whole time?
- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

CONF20. Ask the following if SX-65 and SX-68=0:
"So this means you only had oral sex the last time you had sex?"
If respondent says "no," go back to SX-65.

- SX-70. Before or during the last time you had sex with this partner, did you use:
[READ CHOICES. CHECK only ONE.]
- Alcohol..... 1 *Skip to SX-71*
- Drugs..... 2
- Both alcohol and drugs..... 3
- Neither one..... 4 } *Skip to SX-71.*
- Refused to answer..... 7 }
- Don't know..... 9 }

- SX-70a. Which drugs did you use? **[DO NOT read choices. Check that apply.]**
- Marijuana 1
- Speedballs (heroin and cocaine together) 2
- Heroin 3
- Crack cocaine..... 4
- Powdered cocaine 5
- Crystal meth (tina, crank, ice) 6
- X or Ecstasy 7
- Special K (ketamine) 8

- GHB 9
- Painkillers (Oxycontin, Vicodin, Percocet) 10
- Downers (Valium, Ativan, Xanax) 11
- Hallucinogens (LSD, mushrooms) 12
- Poppers 13
- Other drug 14
- Refused to answer..... 77
- Don't know..... 99

- SX-71. The last time you had sex with this partner, did you know his HIV status?
- No..... 0 **Skip to SX-72**
 - Yes..... 1
 - Refused to answer..... 7 **Skip to SX-72**

- SX-71a. What was his HIV status?
- HIV-negative..... 1
 - HIV-positive..... 2
 - Indeterminate..... 3
 - Refused to answer..... 7

- SX-72. Was this partner younger than you, older than you, or the same age as you?
- Younger 0 **→ Skip to SX-73**
 - Older 1
 - Same age 2
 - Refused to answer..... 7
 - Don't know..... 9
- } Skip to SX-73**

SX-72a. What was his age? _____ **[777 = Refused, 999 = Don't know]**

SX-72b. Which of the following best describes his racial or ethnic background? **[READ choices. Choose one.]**

- American Indian or Alaska Native..... 1
- Asian 2
- Black or African American 3
- Hispanic or Latino..... 4
- Native Hawaiian or Other Pacific Islander..... 5
- White..... 6
- Refused to answer..... 7
- Don't know..... 9

SX-73. As far as you know, has this partner ever injected drugs like heroin, cocaine, or speed? Would you say he: **[READ CHOICES. Check only ONE.]**

- Definitely did not..... 0
- Probably did not..... 1
- Probably did..... 2
- Definitely did 3
- Refused to answer..... 7
- Don't know..... 9

SX-74. As far as you know, has this partner ever used crack cocaine? Would you say he: **[READ CHOICES. Check only ONE.]**

- Definitely did not..... 0
- Probably did not..... 1
- Probably did..... 2
- Definitely did 3
- Refused to answer..... 7
- Don't know..... 9

SX-75. As far as you know, has this partner ever been in prison or jail for more than 24 hours? Would you say he: **[READ CHOICES. Check only ONE.]**

- Definitely did not..... 0
- Probably did not..... 1

- Probably did..... 2
- Definitely did 3
- Refused to answer..... 7
- Don't know..... 9

SX-76. As far as you know, has this partner ever had sex with other men?
 Would you say he: **[READ CHOICES. Check only ONE.]**

- Definitely did not..... 0
- Probably did not..... 1
- Probably did..... 2
- Definitely did 3
- Refused to answer..... 7
- Don't know..... 9

SX-77. How long have you been having a sexual relationship with this partner? (Please tell me how many days, months, or years). **[Interviewer: If “one night stand,” enter 0.]**

of Days: ___ ___

of Months: ___ ___

of Years: ___ ___

[Refused = 777, Don't know = 999]

**If SX-77 > 12 months, 777, or 999, skip to SX-79. If SX-77 ≤ 12 months, skip to SX-80.
 If SX-77=0, skip to SX-80.**

SX-78. As far as you know, during the time you were having a sexual relationship with this partner, did he have sex with other people? Would you say he: **[READ CHOICES. Check only ONE.]**

- Definitely did not..... 0
- Probably did not..... 1
- Probably did..... 2
- Definitely did 3
- Refused to answer..... 7
- Don't know..... 9

SX-78a. During the time you were having a sexual relationship with this partner, did you have sex with other people?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

SX-79. As far as you know, during the past 12 months when you were having a sexual relationship with this partner, did he have sex with other people? Would you say he: **[READ CHOICES. Check only ONE.]**

- Definitely did not..... 0
- Probably did not..... 1
- Probably did..... 2
- Definitely did 3
- Refused to answer..... 7
- Don't know..... 9

SX-79a. During the past 12 months when you were having a sexual relationship with this partner, did you have sex with other people?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

Female Sex Partners (Female Respondents)

SX-80. Now I'm going to ask you about having sex with other women. In the past 12 months, with how many different women have you had sex?

[Refused = 7777, Don't know = 9999] _____

ALCOHOL USE HISTORY (AL)

SAY: The next questions are about alcohol use. Please remember your answers will be kept private. For these questions, "a drink of alcohol" means a 12 oz beer, a 5 oz glass of wine, or a 1.5 oz shot of liquor. **SHOW RESPONDENT FLASHCARD L (PICTURE OF ALCOHOL DRINK SIZE)**

AL-1. In the past 12 months, did you drink any alcohol such as beer, wine, malt liquor, or hard liquor?

- No..... 0  *Skip to Say Box before ID-1*
- Yes..... 1
- Refused to answer..... 7  *Skip to Say Box before ID-1*
- Don't know..... 9

AL-2. In the past 12 months, how often did you have 5 or more alcoholic drinks in one sitting? [**4 or more drinks if respondent is female.**] **GIVE RESPONDENT FLASHCARD K. READ CHOICES. CHECK only ONE.**

- Never..... 0
- More than once a day..... 1
- Once a day..... 2
- More than once a week..... 3
- Once a week..... 4
- More than once a month..... 5
- Once a month..... 6
- Less than once a month..... 7
- Refused to answer..... 77
- Don't know..... 99

AL-3. The next questions are about drinking alcohol during the past 30 days, that is, since the [insert day of current month] of last month. During the past 30 days, on how many days did you drink any alcohol?

[77 = Refused, 99 = Don't know] — —

If AL-3 in (0, 77, 99), skip to Say Box before ID-1.

AL-4. During the past 30 days, on the days when you drank alcohol, how many drinks did you usually have? (*Interviewer: The number of drinks must be greater than 0.*)

[77 = Refused, 99 = Don't know] — —

AL-5. During the past 30 days, how many times did you have 5 or more alcoholic drinks in one sitting?
[4 or more drinks if respondent is female.]

[77 = Refused, 99 = Don't know] — —

DRUG USE HISTORY

Injection Drug Use (ID)

SAY: The next questions are about injection drug use. This means injecting drugs yourself or having someone who isn't a health care provider inject you. Please remember your answers will be kept private.

FOR NHBS-MSM AND NHBS-HET, ASK ID-1

FOR NHBS-IDU, GO TO ID-1a

ID-1. Have you ever in your life shot up or injected any drugs other than those prescribed for you? By shooting up, I mean anytime you might have used drugs with a needle, either by mainlining, skin popping, or muscling.

- No..... 0 → *Skip to Say Box before ND-1*
- Yes..... 1
- Refused to answer..... 7 } *Skip to Say Box before ND-1*
- Don't know..... 9 }

ID-1a. Think back to the very first time you injected any drugs, other than those prescribed for you. How old were you when you first injected any drug?

[77 = Refused, 99 = Don't know] _ _

ID-1b. When was the last time you injected any drug? That is, how many days or months or years ago did you last inject?

[Interviewer: If respondent answers today, enter "000" in # of Days field]

of Days: _ _ _

of Months: _ _ _

of Years: _ _ _

[Refused = 777, Don't know = 999]

***If NHBS-MSM or NHBS-HET and ID-1b > 12 months, skip to Say Box before ND-1.
If NHBS-IDU AND ID-1b > 12 months, skip to END of questionnaire.***

SAY: The next questions are about injection drug use in the past 12 months. When I ask you about "needles," I'm talking about needles and syringes.

ID-2. In the past 12 months, on average, how often did you inject? **[GIVE RESPONDENT FLASHCARD K. READ CHOICES. CHOOSE only ONE.]**

- Never..... 0
- More than once a day..... 1
- Once a day..... 2
- More than once a week..... 3
- Once a week..... 4
- More than once a month..... 5
- Once a month..... 6
- Less than once a month..... 7
- Refused to answer..... 77
- Don't know..... 99

SAY: I'm going to read you a list of drugs. For each drug I mention, please tell me how often you injected it in the past 12 months. **GIVE RESPONDENT FLASHCARD K**

ID-3. How often did you inject... **READ EACH DRUG CHOICE. CHOOSE ONLY ONE RESPONSE PER TYPE OF DRUG**

	Never	More than once a day	Once a day	More than once a week	Once a week	More than once a month	Once a month	Less than once a month	Refused to answer
a. Speedball (heroin & cocaine together)	00	01	02	03	04	05	06	07	77
b. Heroin, by itself	00	01	02	03	04	05	06	07	77
c. Powdered cocaine , by itself	00	01	02	03	04	05	06	07	77
d. Crack cocaine	00	01	02	03	04	05	06	07	77
e. Crystal meth (tina, crank, or ice)	00	01	02	03	04	05	06	07	77
f. Oxycontin	00	01	02	03	04	05	06	07	77

ID-3g1. Did you inject any other drugs in the past 12 months?

- No..... 0 **Skip to SAY box before ID-4**
- Yes..... 1
- Refused to answer..... 7 **Skip to SAY box before ID-4**
- Don't know..... 9

Specify other drug _____

ID-3g2. How often did you inject *[Interviewer: insert other drug specified]*:

- | | Never | More than once a day | Once a day | More than once a week | Once a week | More than once a month | Once a month | Less than once a month | Refused to answer |
|------------------|-------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|-----------------------------|
| g. (Other drug). | <input type="checkbox"/> 00.. | <input type="checkbox"/> 01..... | <input type="checkbox"/> 02..... | <input type="checkbox"/> 03..... | <input type="checkbox"/> 04..... | <input type="checkbox"/> 05..... | <input type="checkbox"/> 06..... | <input type="checkbox"/> 07..... | <input type="checkbox"/> 77 |

ID-4. In the past 12 months when you injected, did you get your needles at any of the following places? **[GIVE RESPONDENT FLASHCARD M; READ ALL CHOICES]**

- | | No | Yes | Refused to answer | Don't know |
|--|--------------------------------|--------------------------------|--------------------------------|----------------------------|
| a. Pharmacy or drug store | <input type="checkbox"/> 0.... | <input type="checkbox"/> 1.... | <input type="checkbox"/> 7.... | <input type="checkbox"/> 9 |
| b. Doctor's office, clinic, or hospital..... | <input type="checkbox"/> 0.... | <input type="checkbox"/> 1.... | <input type="checkbox"/> 7.... | <input type="checkbox"/> 9 |
| c. Friend, acquaintance, relative, or sex partner..... | <input type="checkbox"/> 0.... | <input type="checkbox"/> 1.... | <input type="checkbox"/> 7.... | <input type="checkbox"/> 9 |
| d. Needle or drug dealer, shooting gallery, hit house, off the street... | <input type="checkbox"/> 0.... | <input type="checkbox"/> 1.... | <input type="checkbox"/> 7.... | <input type="checkbox"/> 9 |
| e. Needle exchange program..... | <input type="checkbox"/> 0.... | <input type="checkbox"/> 1.... | <input type="checkbox"/> 7.... | <input type="checkbox"/> 9 |
| f. Some other place.....
(Specify _____) | <input type="checkbox"/> 0.... | <input type="checkbox"/> 1.... | <input type="checkbox"/> 7.... | <input type="checkbox"/> 9 |

ID-5. In the past 12 months when you injected, how often did you use a new, sterile needle? By a new, sterile needle, I mean a needle never used before by anyone, even you. **[GIVE RESPONDENT FLASHCARD N, READ CHOICES. CHECK only ONE.]**

- Never..... 0
- Rarely..... 1
- About half the time..... 2
- Most of the time..... 3
- Always..... 4
- Refused to answer..... 7
- Don't know..... 9

SAY: Next, I'm going to ask you about your injecting behaviors in the past 12 months.

ID-6. In the past 12 months, with how many people did you use a needle after they injected with it?

[Refused = 777, Don't know = 999] _ _ _

ID-7. In the past 12 months, with how many people did you use the same cooker, cotton, or water that they had already used. By “water,” I mean water for rinsing needles or preparing drugs.

[Refused = 777, Don't know = 999] _ _ _

ID-8. In the past 12 months, with how many people did you use drugs that had been divided with a syringe that they had already used?

[Refused = 777, Don't know = 999] _ _ _

If ID-6 ≥ 1, ask ID-9

ID-9. In the past 12 months, how often did you use needles that someone else had already injected with? [GIVE RESPONDENT FLASHCARD N, READ CHOICES. CHECK only ONE]

- Never..... 0
- Rarely..... 1
- About half the time..... 2
- Most of the time..... 3
- Always..... 4
- Refused to answer..... 7
- Don't know..... 9

For NHBS-IDU, ask ID-10 through ID-12 then skip to ID-14

If ID-7 ≥ 1, ask ID-10– ID-12

ID-10. In the past 12 months when you injected, how often did you use a cooker that someone else had already used? [GIVE RESPONDENT FLASHCARD N, READ CHOICES, CHECK only ONE.]

- Never..... 0
- Rarely..... 1
- About half the time..... 2
- Most of the time..... 3
- Always..... 4
- Refused to answer..... 7
- Don't know..... 9

ID-11. In the past 12 months when you injected, how often did you use a cotton that someone else had already used? **[GIVE RESPONDENT FLASHCARD N, READ CHOICES, CHECK only ONE.]**

- Never..... 0
- Rarely..... 1
- About half the time..... 2
- Most of the time..... 3
- Always..... 4
- Refused to answer..... 7
- Don't know..... 9

ID-12. In the past 12 months when you injected, how often did you use water that someone else had already used? **[GIVE RESPONDENT FLASHCARD N, READ CHOICES, CHECK only ONE]**

- Never..... 0
- Rarely..... 1
- About half the time..... 2
- Most of the time..... 3
- Always..... 4
- Refused to answer..... 7
- Don't know..... 9

FOR NHBS-MSM AND NHBS-HET, ASK ID-13

If ID-7 ≥ 1, ask ID-13

ID-13. In the past 12 months when you injected, how often did you use cookers, cottons, or water that someone else had already used? **[GIVE RESPONDENT FLASHCARD N, READ CHOICES, CHECK only ONE.]**

- Never..... 0
- Rarely..... 1
- About half the time..... 2
- Most of the time..... 3
- Always..... 4
- Refused to answer..... 7
- Don't know..... 9

If ID-8 ≥ 1, ask ID-14

ID-14. In the past 12 months when you injected, how often did you use drugs that had been divided with a syringe that someone else had already injected with? **[GIVE RESPONDENT FLASHCARD N, READ CHOICES. CHECK only ONE.]**

- Never..... 0
- Rarely..... 1
- About half the time..... 2
- Most of the time..... 3
- Always..... 4
- Refused to answer..... 7
- Don't know..... 9

If ID-6= 0, DK, or REF and
If ID-7= 0, DK, or REF and
If ID-8= 0, DK, or REF
then skip to the non-injection drug use section (ND)

SAY: Now I'd like you to think about the **last time** you injected with someone.
 By "injecting with someone," I mean you shared drugs or equipment, or both with at least one other person that you were with when you injected.

ID-15. When was the last time you injected with someone?

[77/7777 = Refused, 99/9999 = Don't know] (M M / Y Y Y Y)

If ID-6=0, Skip to ID-17

ID-16. The last time you injected with someone, did you use a needle after anyone else had already injected with it?

- No..... 0
- Yes..... 1 **Skip to ID-17**
- Refused to answer..... 7
- Don't know..... 9

- ID-16a. Did you use a new sterile needle to inject?
- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

If ID-7=0, Skip to ID-18

- ID-17. The last time you injected with someone, did you use a cooker, cotton, or water that anyone else had already used?
- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

If ID-8=0, Skip to ID-19

- ID-18. The last time you injected with someone, did you use drugs that had been divided with a syringe that anyone else had already injected with?
- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

SAY: The next questions are about this last person you injected with.

- ID-19. Is this person male or female?
- Male..... 1
- Female..... 2 **→** *Skip to ID-21*
- Other (specify _____)..... 3

ID-20. As far as you know, has this person ever had sex with another man? Would you say he:
[READ CHOICES. Check only ONE.]

- Definitely did not..... 0
- Probably did not..... 1
- Probably did..... 2
- Definitely did 3
- Refused to answer..... 7
- Don't know..... 9

ID-21. The last time you injected with this person, did you know their HIV status?

- No..... 0 **Skip to ID-22**
- Yes..... 1
- Refused to answer..... 7 **Skip to ID-22**

ID-21a. What was their HIV status?

- HIV-negative..... 1
- HIV-positive..... 2
- Indeterminate..... 3
- Refused to answer..... 7

ID-22. The last time you injected with this person, did you know if they had been tested for hepatitis C?

- No..... 0 **Skip to ID-23**
- Yes..... 1
- Refused to answer..... 7 **Skip to ID-23**

ID-22a. What was the result of their hepatitis C test?

- Negative..... 1
- Positive..... 2
- Refused to answer..... 7
- Don't know..... 9

ID-23. Which of the following best describes your relationship to this person? Would you say this person was a: **[GIVE RESPONDENT FLASHCARD O. READ CHOICES, CHECK only ONE.]**

- Sex partner 1
- Friend or acquaintance 2
- Relative 3
- Needle or drug dealer..... 4
- Stranger..... 5
- Other (specify _____)..... 6
- Refused to answer..... 7
- Don't know..... 9

Non-Injection Drug Use (ND)

SAY: Now I'm going to ask you about drugs that you may have used but did not inject. I will refer to these as non-injection drugs. This includes drugs like marijuana, crystal meth, cocaine, crack, club drugs, painkillers, or poppers.

ND-1. In the past 12 months, have you used any non-injection drugs, other than those prescribed for you?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

If ES9=2 and ND-1 in (0, 7, 9), skip to Say Box before TX-1.
If ES9=1 and ND-1 in (0, 7, 9), skip to ND-3.

SAY: I'm going to read you a list of drugs. For each drug I mention, please tell me how often you used it in the past 12 months. **Do not** include drugs you injected or drugs that were prescribed for you. **GIVE RESPONDENT FLASHCARD K.**

ND-2. How often did you use...**READ EACH DRUG CHOICE. CHOOSE ONLY ONE RESPONSE PER TYPE OF DRUG.**

- | | Never | More than once a day | Once a day | More than once a week | Once a week | More than once a month | Once a month | Less than once a month | Refused to answer |
|--|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|
| a. Marijuana..... | <input type="checkbox"/> 00 | <input type="checkbox"/> 01 | <input type="checkbox"/> 02 | <input type="checkbox"/> 03 | <input type="checkbox"/> 04 | <input type="checkbox"/> 05 | <input type="checkbox"/> 06 | <input type="checkbox"/> 07 | <input type="checkbox"/> 77 |
| b. Crystal meth (tina, crank, or ice)..... | <input type="checkbox"/> 00 | <input type="checkbox"/> 01 | <input type="checkbox"/> 02 | <input type="checkbox"/> 03 | <input type="checkbox"/> 04 | <input type="checkbox"/> 05 | <input type="checkbox"/> 06 | <input type="checkbox"/> 07 | <input type="checkbox"/> 77 |
| c. Crack cocaine..... | <input type="checkbox"/> 00 | <input type="checkbox"/> 01 | <input type="checkbox"/> 02 | <input type="checkbox"/> 03 | <input type="checkbox"/> 04 | <input type="checkbox"/> 05 | <input type="checkbox"/> 06 | <input type="checkbox"/> 07 | <input type="checkbox"/> 77 |
| d. Powdered cocaine that is smoked or snorted..... | <input type="checkbox"/> 00 | <input type="checkbox"/> 01 | <input type="checkbox"/> 02 | <input type="checkbox"/> 03 | <input type="checkbox"/> 04 | <input type="checkbox"/> 05 | <input type="checkbox"/> 06 | <input type="checkbox"/> 07 | <input type="checkbox"/> 77 |
| e. Downers such as Valium, Ativan, or Xanax..... | <input type="checkbox"/> 00 | <input type="checkbox"/> 01 | <input type="checkbox"/> 02 | <input type="checkbox"/> 03 | <input type="checkbox"/> 04 | <input type="checkbox"/> 05 | <input type="checkbox"/> 06 | <input type="checkbox"/> 07 | <input type="checkbox"/> 77 |
| f. Painkillers such as Oxycontin, Vicodin, or Percocet, | <input type="checkbox"/> 00 | <input type="checkbox"/> 01 | <input type="checkbox"/> 02 | <input type="checkbox"/> 03 | <input type="checkbox"/> 04 | <input type="checkbox"/> 05 | <input type="checkbox"/> 06 | <input type="checkbox"/> 07 | <input type="checkbox"/> 77 |
| g. Hallucinogens such as LSD or mushrooms..... | <input type="checkbox"/> 00 | <input type="checkbox"/> 01 | <input type="checkbox"/> 02 | <input type="checkbox"/> 03 | <input type="checkbox"/> 04 | <input type="checkbox"/> 05 | <input type="checkbox"/> 06 | <input type="checkbox"/> 07 | <input type="checkbox"/> 77 |
| h. X or Ecstasy..... | <input type="checkbox"/> 00 | <input type="checkbox"/> 01 | <input type="checkbox"/> 02 | <input type="checkbox"/> 03 | <input type="checkbox"/> 04 | <input type="checkbox"/> 05 | <input type="checkbox"/> 06 | <input type="checkbox"/> 07 | <input type="checkbox"/> 77 |
| i. Heroin that is smoked or snorted..... | <input type="checkbox"/> 00 | <input type="checkbox"/> 01 | <input type="checkbox"/> 02 | <input type="checkbox"/> 03 | <input type="checkbox"/> 04 | <input type="checkbox"/> 05 | <input type="checkbox"/> 06 | <input type="checkbox"/> 07 | <input type="checkbox"/> 77 |

If NHBS-MSM, ask ND-2j – ND-2l

- | | | | | | | | | | |
|-------------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|
| j. Poppers (amyl nitrate)... | <input type="checkbox"/> 00 | <input type="checkbox"/> 01 | <input type="checkbox"/> 02 | <input type="checkbox"/> 03 | <input type="checkbox"/> 04 | <input type="checkbox"/> 05 | <input type="checkbox"/> 06 | <input type="checkbox"/> 07 | <input type="checkbox"/> 77 |
| k. GHB..... | <input type="checkbox"/> 00 | <input type="checkbox"/> 01 | <input type="checkbox"/> 02 | <input type="checkbox"/> 03 | <input type="checkbox"/> 04 | <input type="checkbox"/> 05 | <input type="checkbox"/> 06 | <input type="checkbox"/> 07 | <input type="checkbox"/> 77 |
| l. Special K (ketamine)..... | <input type="checkbox"/> 00 | <input type="checkbox"/> 01 | <input type="checkbox"/> 02 | <input type="checkbox"/> 03 | <input type="checkbox"/> 04 | <input type="checkbox"/> 05 | <input type="checkbox"/> 06 | <input type="checkbox"/> 07 | <input type="checkbox"/> 77 |

ND-2m1. In the past 12 months have you used any other non-injection drugs?

No..... 0 → *Skip to ND-3*

Yes..... 1

Refused to answer..... 7 } *Skip to ND-3*

Don't know..... 9 }

Specify other drug _____

ND-2m2. How often did you use:

	Never	More than once a day	Once a day	More than once a week	Once a week	More than once a month	Once a month	Less than once a month	Refused to answer
m. (Other drug).	<input type="checkbox"/> 00..	<input type="checkbox"/> 01.....	<input type="checkbox"/> 02.....	<input type="checkbox"/> 03.....	<input type="checkbox"/> 04.....	<input type="checkbox"/> 05.....	<input type="checkbox"/> 06.....	<input type="checkbox"/> 07.....	<input type="checkbox"/> 77

If Respondent is not male (ES9 ≠ 1), skip to Say Box before TX-1.

ND-3. In the past 12 months, have you used Viagra, Levitra or Cialis?

No..... 0

Yes..... 1

Refused to answer..... 7

Don't know..... 9

If TX-1 in (0, 7, 9), skip to Say Box before TX-1.

ND-3a. Did you use it to treat erectile dysfunction?

No..... 0

Yes..... 1

Refused to answer..... 7

Don't know..... 9

If Respondent is male (ES9 =1) AND ID-3e or ND-2b are not 0 or 77, ask ND-3b. Otherwise, skip to Say Box before TX-1.

ND-3b. You told me that you used crystal meth (tina, crank, ice). In the past 12 months, did you use Viagra, Levitra or Cialis at the same time you used crystal meth?

No..... 0

Yes..... 1

Refused to answer..... 7

Don't know..... 9

ALCOHOL AND DRUG TREATMENT

SAY: Next, I'm going to ask you about alcohol and drug treatment programs. These include out-patient, in-patient, residential, detox, methadone treatment, or 12-step programs.

TX-1. Have you ever participated in an alcohol treatment program?

- No..... 0
Yes..... 1
Refused to answer..... 7
Don't know..... 9

If TX-1=0, skip to TX-1b. If TX-1 in (7, 9), skip to TX-2.

TX-1a. Have you participated in an alcohol treatment program in the past 12 months?

- No..... 0
Yes..... 1
Refused to answer..... 7
Don't know..... 9

TX-1b. In the past 12 months, did you try to get into an alcohol treatment program but were unable to?

- No..... 0
Yes..... 1
Refused to answer..... 7
Don't know..... 9

TX-2. Have you ever participated in a drug treatment program?

- No..... 0
Yes..... 1
Refused to answer..... 7
Don't know..... 9

If TX-2=0, skip to TX-2b. If TX-2 in (7, 9), skip to Say Box before HT-1

TX-2a. Have you participated in a drug treatment program in the past 12 months?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

TX-2b. In the past 12 months, did you try to get into a drug treatment program but were unable to?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

HIV TESTING EXPERIENCES

SAY: Now I'm going to ask you a few questions about getting tested for HIV. Remember, an HIV test checks whether someone has the virus that causes AIDS.

- HT-1. Have you ever been tested for HIV?
- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

***If HT-1=0, skip to HT-6.
If HT-1 in (7, 9), Skip to Say Box before HT-9.***

- HT-2. When did you have your first HIV test?
- [77/7777 = Refused, 99/9999 = Don't know] $\frac{\text{M M}}{\text{Y Y Y Y}}$

CONF21. INTERVIEWER INSTRUCTIONS:

HIV testing was not widely available before 1985. Please confirm the year. Is [TST1TSTY] correct?

- Yes..... 1 Go to next question***
- No..... 0 Loop back to put in the correct year***

- HT-3. In the past 2 years, that is, since [*insert calculated month and year*], how many times have you been tested for HIV?
- _____

[Refused = 777, Don't know = 999] ➔ If 0, 777, or 999, skip to HT-4

- HT-4. When did you have your most recent HIV test?
- [77/7777 = Refused, 99/9999 = Don't know] $\frac{\text{M M}}{\text{Y Y Y Y}}$

If Auto3 - HT-4 is > 5 years ago, skip to HT-4c.

CONF22. INTERVIEWER INSTRUCTIONS:

HIV testing was not widely available before 1985. Please confirm the year. Is &[RCNTTSTY] correct?

Yes..... ₁ Go to next question

No..... ₀ Loop back to put in the correct year

HT-4a. When you got tested in ____/____ [*insert date from HT-4*], where did you get tested?

Testing Site: _____

[Write down the site name and classify it from the list of choices below. Probe with additional questions if necessary. DO NOT read choices. Choose only ONE site type.]

- HIV counseling and testing site..... 01
- HIV/AIDS street outreach program/Mobile Unit... 02
- Drug treatment program..... 03
- Needle exchange program..... 04
- Correctional facility (jail or prison)..... 05
- Family planning or obstetrics clinic..... 06
- Public health clinic/ Community health center 07
- Private doctor's office (including HMO)..... 08
- Emergency room..... 09
- Hospital (inpatient)..... 10
- At home..... 11
- Other..... 12
- Refused..... 77
- Don't know..... 99

HT-4b. When you got tested in ____/____ [*insert date from HT-4*], was it a rapid test where you could get your results within a couple of hours?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

- HT-4c. What was the result of your most recent HIV test? *[DO NOT Read choices, check only ONE.]*
- Negative..... 1
 - Positive..... 2
 - Never obtained results..... 3
 - Indeterminate..... 4
 - Refused to answer..... 7
 - Don't know..... 9

***If HT-4c=1, go to Logic check before HT-6. If HT-4c=2, skip to HT-7.
If HT-4c in (7, 9), go to Logic Check before HT-6.***

- HT-5. Before your test in ____/____ *[insert date from HT-4]*, did you ever test positive for HIV?
- No..... 0
 - Yes..... 1 ***Skip to HT-7a***
 - Refused to answer..... 7
 - Don't know..... 9

INTERVIEWER INSTRUCTIONS: Refer to HT-4. LAST HIV TEST WAS DONE (Check one):

<i>≤ 12 months ago.....</i> <input type="checkbox"/>	<i>SAY Box before HT-9</i>
<i>> 12 months ago.....</i> <input type="checkbox"/>	<i>Go to next question</i>
<i>Date of last test Don't know/Refused... </i> <input type="checkbox"/>	<i>Go to SAY Box before HT-9</i>

[PERSONS WHO HAVE NEVER TESTED HIV+ AND HAVE NOT TESTED FOR HIV IN THE PAST 12 MONTHS]

- HT-6. I'm going to read you a list of reasons why some people have not been tested for HIV. Which of these best describes the most important reason you have not been tested for HIV in the past 12 months? ***[READ CHOICES. CHOOSE only ONE.]***
- You think you are at low risk for HIV infection?..... 1
 - You were afraid of finding out that you had HIV?..... 2
 - You didn't have time?..... 3
 - Some other reason?..... 4
 - No particular reason..... 5
 - Refused to answer..... 7
 - Don't know..... 9

If HT-6 in ≠ 4, go to Say Box before HT-9.

HT-6a. What was the most important reason you have not been tested for HIV in the past 12 months?

Go to Say Box before HT-9.

[PERSONS WHO HAVE TESTED HIV POSITIVE]

HT-7. Was your test in ____/____ [insert date from HT-4] your first positive test?

No..... 0

Yes..... 1

Refused to answer..... 7

Don't know..... 9

} Skip to HT-7b

HT-7a. When did you first test positive?

[77/7777 = Refused, 99/9999 = Don't know]

(M M / Y Y Y Y)

CONF23. INTERVIEWER INSTRUCTIONS:

HIV testing was not widely available before 1985. Please confirm the year. Is [POS1STDY] correct?

Yes..... 1 **Go to next question**

No..... 0 **Loop back to put in the correct year**

HT-7b. After you tested positive, were you asked by someone from the health department or your health care provider to give the names of your sex or drug use partners so they could be notified that they may have been exposed to HIV?

No..... 0

Yes..... 1

Refused to answer..... 7

Don't know..... 9

If Q133e in (0, 7, 9), skip to HT-7d.

HT-7c. Did you give the names or contact information of any of your partners when asked?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

HT-7d. Before your first positive test in ____ / ____ [insert date from HT-4 or HT-7a], did you ever have a negative HIV test? (By negative HIV test, I mean the test showed you did not have HIV infection.)

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

If HT-7d in (0, 7, 9), skip to HT-7e.

HT-7d.1 What was the month and year that you got your last negative HIV test? Tell me when you got your last test, not when you got your results.

[77/7777 = Refused, 99/9999 = Don't know] (M M / Y Y Y Y)

HT-7e. In the 2 years before your first positive test in ____ / ____ [insert date from HT-4 or HT-7a], how many times did you get tested for HIV? Don't include your first positive test in that total number.

[Refused = 7777, Don't know = 9999] _ _ _ _

HT-7f. Have you ever been seen by a doctor, nurse, or other health care provider for a medical evaluation or care related to your HIV infection?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

If HT-7f = 1, skip to HT-7g.

If HT-7f in (7, 9), skip to Say Box before HT-8b.

HT-7f.1. What is the main reason you have never gone to a health care provider for a medical evaluation or care related to your HIV infection? *[DO NOT read choices. Choose only ONE reason.]*

- Feel good, don't need to go 01
- Don't want to think about being HIV positive/Denial..... 02
- Didn't have money or insurance..... 03
- Inconvenient (location/hours/time, etc.)..... 04
- Forgot to go/Missed appointment..... 05
- Drinking or using drugs..... 06
- Appointment pending..... 07
- Other..... 08
- Refused..... 77
- Don't know..... 99

If HT-7f.1=8, ask HT-7f.2. Otherwise, skip to Say Box before HT-8b.

HT-7f.2. *Interviewer: Type in other reason Respondent never sought HIV care.*

Skip to Say Box before HT-8b.

HT-7g. When did you first go to your health care provider after learning you had HIV?

[77/7777=Refused, 99/9999 = Don't know] (M M / Y Y Y Y)

INTERVIEWER INSTRUCTIONS: Refer to date of first positive HIV test (HT-4or HT-7a)

<i>≤ 3 months before first provider visit</i>	<i>Skip to HT-7i</i>
<i>> 3 months before first provider visit</i>	<i>Go to next question</i>
<i>Interval cannot be determined (date missing)</i>	<i>Skip to HT-7i</i>

If first positive test result was > 3 years before [date of interview], skip to HT-7i

HT-7h. Some people go to a health care provider soon after learning they are positive; others do not. What is the main reason you didn't go to a health care provider soon after you learned of your HIV infection? *[DO NOT read choices. Choose only ONE reason.]*

- Felt good, didn't need to go 01
- Didn't want to think about being HIV positive/Denial..... 02
- Didn't have money or insurance..... 03
- Inconvenient (location/hours/time, etc.)..... 04
- Forgot to go/Missed appointment..... 05
- Drinking or using drugs..... 06
- Unable to get an earlier appointment..... 07
- Other..... 08
- Refused..... 77
- Don't know..... 99

If HT-7h = 8, ask HT-7h.1. Otherwise, go to HT-7i.

HT-7h.1 ***Interviewer: Type in other reason Respondent did not seek HIV care soon after diagnosis:***

HT-7i. When did you last go to your health care provider for HIV care?

[77/7777=Refused, 99/9999 = Don't know] (M M / Y Y Y Y)

INTERVIEWER INSTRUCTIONS:

<i>≤ 6 months since last provider visit</i>	<i>Skip to HT-8</i>
<i>> 6 months since last provider visit</i>	<i>Go to next question</i>
<i>Interval cannot be determined (date missing)</i>	<i>Skip to HT-8</i>

HT-7j. What is the main reason you have not gone to a health care provider for HIV care in the past 6 months? *[DO NOT Read reason types. Choose only ONE reason.]*

- Felt good, didn't need to go..... 01
- Don't want to think about being HIV positive/Denial..... 02
- Didn't have money or insurance..... 03
- Inconvenient (location/hours/time, etc.)..... 04
- Forgot to go/Missed appointment..... 5

- Drinking or using drugs..... 06
- Appointment pending..... 07
- Other..... 08
- Refused..... 77
- Don't know..... 99

If HT-7j = 8, ask HT-7j.1. Otherwise, go to HT-8.

HT-7j.1. **Interviewer: Type in other reason Respondent has not sought HIV care in past 6 months:**

- HT-8. Are you currently taking antiretroviral medicines to treat your HIV infection?
- No..... 0
 - Yes..... 1
 - Refused to answer..... 7
 - Don't know..... 9

If HT-8 in (1, 7, 9), skip to Say Box before HT-8b.

- HT-8a. What is the main reason you are not currently taking any antiretroviral medicines? **[DO NOT read reason types. Choose only ONE reason.]**
- Feel good, don't need them..... 01
 - CD4 count and viral load are good..... 02
 - Doctor advised to delay treatment..... 03
 - Don't want to think about being HIV positive./Denial..... 04
 - Worried about side effects 05
 - Don't have money or insurance..... 06
 - Drinking or using drugs..... 07
 - Recently into medical care..... 08
 - Other..... 09
 - Refused..... 77
 - Don't know..... 99

If HT-8a = 9, ask HT-8a.1. Otherwise, go to Say Box before HT-8b.

HT-8a.1 ***Interviewer: Type in other reason Respondent is not currently taking ARVs:***

SAY: Researchers are studying whether antiretroviral medicines could possibly be taken to prevent HIV infection.

HT-8b. Before today, have you ever heard of people who do not have HIV taking antiretroviral medicines, to keep from getting HIV?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

If HT-8 ≠ 1, skip to Say Box before HT-14.

HT-8c. In the past 12 months, have you given your antiretroviral medicines to a sex partner who was HIV-negative because you thought it might keep them from getting HIV?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

Skip to SAY Box before HT-14

FOR PARTICIPANTS WHO HAVE NOT PREVIOUSLY TESTED HIV+:

SAY: Researchers are studying whether anti-HIV medicine (also called antiretrovirals)-- a pill -- could possibly be taken to prevent HIV infection.

HT-9. Before today, have you ever heard of people who do not have HIV taking anti-HIV medicines, to keep from getting HIV?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

HT-10. In the past 12 months, have you taken anti-HIV medicines after sex because you thought it would keep you from getting HIV?

- No..... 0
 Yes..... 1
 Refused to answer..... 7
 Don't know..... 9

HT-11. In the past 12 months, have you taken anti-HIV medicines before sex because you thought it would keep you from getting HIV?

- No..... 0
 Yes..... 1
 Refused to answer..... 7
 Don't know..... 9

If participant has not taken PEP or PrEP in the past 12 months, skip to HT-14.

HT-12. Please tell me if you got any of the anti-HIV medicines you took from the following people or places. Did you get them from...**[GIVE RESPONDENT FLASHCARD P. READ ALL CHOICES.]**

	No	Yes	Refused to answer	Don't know
a. Doctor or other health care provider	0	1	7	9
b. Sex partner, friend, relative, or acquaintance	0	1	7	9
c. Internet	0	1	7	9
d. Some other place (<i>Specify</i> _____)	0	1	7	9

HT-12d.1. **Interviewer:** *Type in other specified place* _____.

HT-13. Would you be willing to take anti-HIV medicines every day to lower your chances of getting HIV?

- No..... 0
 Yes..... 1
 Refused to answer..... 7
 Don't know..... 9

FOR ALL PARTICIPANTS:

SAY: Now I'm going to read you some statements. Please tell me how strongly you agree or disagree with each statement, using the options on this card. *[Give participant Flashcard G]*

HT-14. The first statement is... Most people in *[project area]* would discriminate against someone with HIV. Do you...*[Read choices. Mark only one.]*

- Strongly agree..... 01
- Agree..... 02
- Neither agree nor disagree..... 03
- Disagree..... 04
- Strongly disagree..... 05
- Refused to answer..... 07
- Don't know..... 09

HT-15. Most people in *[project area]* would support the rights of a person with HIV to live and work wherever they wanted to. Do you...*[Read choices. Mark only one.]*

- Strongly agree..... 01
- Agree..... 02
- Neither agree nor disagree..... 03
- Disagree..... 04
- Strongly disagree..... 05
- Refused to answer..... 07
- Don't know..... 09

HT-16. Most people in *[project area]* would not be friends with someone with HIV. Do you...*[Read choices. Mark only one.]*

- Strongly agree..... 01
- Agree..... 02
- Neither agree nor disagree..... 03
- Disagree..... 04
- Strongly disagree..... 05
- Refused to answer..... 07
- Don't know..... 09

HT-17. Most people in *[project area]* think that people who got HIV through sex or drug use have gotten what they deserve. Do you...*[Read choices. Mark only one.]*

- Strongly agree..... 01
- Agree..... 02
- Neither agree nor disagree..... 03
- Disagree..... 04
- Strongly disagree..... 05
- Refused to answer..... 07
- Don't know..... 09

HEALTH CONDITIONS (HC)

SAY: Next, I'd like to ask you some questions about your health.

If Respondent is Male (ES9 =1), ask HC-1

- HC-1. Have you been circumcised?
- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

SAY: The next questions are about hepatitis, an infection of the liver.

- HC-2. Has a doctor, nurse or other health care provider ever told you that you had hepatitis?
- No..... 0 → *Skip to HC-5*
- Yes..... 1
- Refused to answer..... 7 } *Skip to HC-5*
- Don't know..... 9 }

- HC-2a. What type or types of hepatitis have you had? [**CHECK ALL THAT APPLY.**]
- Hepatitis A..... 0
- Hepatitis B..... 1
- Hepatitis C..... 2
- Other..... 3
- If Other:** Specify _____
- Refused to answer..... 7
- Don't know..... 9

If HC-2a in (0, 3, 7, 9), skip to HC-5.

If participant reports history of hepatitis B infection (HC-2a=1), ask HC-3.

If participant reports history of hepatitis C infection (HC-2a=2), ask HC-4a thru HC-4c).

HC-3. Have you ever taken medicine to treat your hepatitis B infection?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

HC-4a. When were you told you had hepatitis C? *[READ CHOICES. CHECK ONE.]*

- 6 months ago or less..... 0
- More than 6 months, but less than 1 year ago..... 1
- At least 1 year but less than 5 years ago 2
- At least 5 years but less than 10 years ago..... 3
- 10 years ago or more..... 4
- Refused to answer..... 7
- Don't know..... 9

HC-4b. Have you ever taken medicine to treat your hepatitis C infection?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

If HC-4b = 0, 7, OR 9, skip to HC-5.

HC-4c. Did your doctor tell you that you were cured of your hepatitis C infection after you finished taking medicine for hepatitis C?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

SAY: Now I'm going to ask you about getting tested for hepatitis.

HC-5. Have you ever had a blood test to check for hepatitis C infection?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

If HC-5 is (0, 7, 9), skip to HC-5b.

HC-5a. When did you have your most recent hepatitis C test? **[READ CHOICES. CHECK only ONE]**

- 6 months ago or less..... 0
- More than 6 months ago, but less than 1 year.... 1
- 1 year ago or more..... 2
- Refused to answer..... 7
- Don't know..... 9

HC-5b. Have you ever had a blood test to check for for hepatitis B?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

If HC-5b in (0,7,9), skip to HC-6.

HC-5c. When did you have your most recent hepatitis B test? **[READ CHOICES. CHECK only ONE]**

- 6 months ago or less..... 0
- More than 6 months ago, but less than 1 year... 1
- 1 year ago or more..... 2
- Refused to answer..... 7
- Don't know..... 9

HC-6. There are vaccines or shots that can prevent some types of hepatitis. Have you ever had a hepatitis vaccine?

- No..... 0  *Skip to
Say box before HC-7*
- Yes..... 1
- Refused to answer..... 7 
- Don't know..... 9 *Skip to
Say box before HC-7*

HC-6a. What type or types of hepatitis vaccine have you had? [**READ CHOICES. CHECK only ONE**]

- Hepatitis A vaccine..... 1
- Hepatitis B vaccine..... 2
- Both Hepatitis A and B vaccines..... 3
- Refused to answer..... 7
- Don't know..... 9

SAY: Now, I'm going to ask you some questions about sexually transmitted diseases, or STDs, other than HIV and hepatitis.

HC-7. Has a doctor or other health care provider **ever** told you that you had genital herpes?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

HC-8. Has a doctor or other health care provider **ever** told you that you had genital warts?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

HC-9. Has a doctor or other health care provider **ever** told you that you had human papillomavirus or HPV?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

HC-10. In the past 12 months, that is, since (__/____), were you **tested** by a doctor or other health care provider for a sexually transmitted disease like gonorrhea, chlamydia, or syphilis? Do **NOT** include tests for HIV or hepatitis.

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

If HC-10 = 0, skip to HC-12.

HC-11. In the past 12 months, that is, since (__/____), were you **tested** for... *[READ choices. CHECK YES or NO for each one.]*

- | | No | Yes | Refused
to answer | Don't
Know |
|-------------------------------------|---------------------------------|--|---------------------------------|----------------------------|
| a. Gonorrhea?..... | <input type="checkbox"/> 0..... | <input checked="" type="checkbox"/> 1..... | <input type="checkbox"/> 7..... | <input type="checkbox"/> 9 |
| b. Chlamydia?..... | <input type="checkbox"/> 0..... | <input checked="" type="checkbox"/> 1..... | <input type="checkbox"/> 7..... | <input type="checkbox"/> 9 |
| c. Syphilis?..... | <input type="checkbox"/> 0..... | <input checked="" type="checkbox"/> 1..... | <input type="checkbox"/> 7..... | <input type="checkbox"/> 9 |
| d. Some other STD (except HIV)?.... | <input type="checkbox"/> 0..... | <input checked="" type="checkbox"/> 1..... | <input type="checkbox"/> 7..... | <input type="checkbox"/> 9 |
| d.1 <i>If Yes: Specify</i> _____ | | | | |

HC-12. In the **past 12 months**, has a doctor or other health care provider told you that you had gonorrhea?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

HC-13. In the **past 12 months**, has a doctor or other health care provider told you that you had Chlamydia?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

HC-14. In the **past 12 months**, has a doctor or other health care provider told you that you had syphilis?

No..... 0

Yes..... 1

Refused to answer..... 7

Don't know..... 9

HC-15. In the **past 12 months**, has a doctor or other health care provider told you that you had any other sexually transmitted disease?

No..... 0

Yes..... 1

Refused to answer..... 7

Don't know..... 9

If HC-15 =0, skip to HC-16

HC-15a. What was that other STD? _____

If participant was ever diagnosed with HPV (HC-9= 1), skip to JT-1.

HC-16. A vaccine to prevent HPV infection is available and is called the HPV shot, cervical cancer vaccine, GARDASIL®, or CERVARIX®. Have you ever received the HPV shot or cervical cancer vaccine?

No..... 0

Yes..... 1

Refused to answer..... 7

Don't know..... 9

If HC-16 in (0, 7, 9), skip to JT-1.

HC-17. How old were you when you received your first dose of the HPV vaccine?

[77= Refused, 99= Don't know] _____

HIV TESTING IN JAIL (JT)

SAY: Now I will ask about experiences you may have had with the criminal justice system. Please remember your answers will be kept private.

JT-1. Have you ever been held in a detention center, jail, or prison for more than 24 hours?

- No..... 0 **→** *Skip to Say Box PA-1*
- Yes..... 1
- Refused to answer..... 7 } *Skip to Say Box PA-1*
- Don't know..... 9 }

JT-1a. During the past 12 months, have you been held in a detention center, jail, or prison, for more than 24 hours??

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

If JT-1a in (0, 7, 9), skip to Say Box before PA-1.

JT-2. During the past 12 months, when you were in detention, jail, or prison, did you get a test for HIV?

- No..... 0 **→** *Skip to JT-3*
- Yes..... 1
- Refused to answer..... 7 } *Skip to JT-3*
- Don't know..... 9 }

JT-2a. During the past 12 months, how many times did you get tested for HIV in detention, jail, or prison?

[77 = Refused, 99 = Don't know] _ _ _

JT-2b. *[If JT-2a > 1 and < 77, autofill with “Think of the last time you were tested for HIV in detention, jail, or prison.”]* Did you get the results of that HIV test?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

JT-3. During the past 12 months, when you were in detention, jail, or prison, did you get a test for hepatitis C?

- No..... 0 → *Skip to Say Box before PA-1*
- Yes..... 1
- Refused to answer..... 7 } *Skip to Say Box before PA-1*
- Don't know..... 9 }

JT-3a. During the past 12 months, how many times did you get tested for hepatitis C in detention, jail, or prison?

[77 = Refused, 99 = Don't know] _ _

JT-3b. *[If JT-3a > 1 and < 77, autofill with “Think of the last time you were tested for hepatitis C in detention, jail, or prison.”]* Did you get the results of that hepatitis C test?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

ASSESSMENT OF PREVENTION ACTIVITIES (PA)

SAY: Next I'd like to ask you about HIV prevention activities that happen around here.

PA-1. In the past 12 months, have you gotten any free condoms, not counting those given to you by a friend, relative, or sex partner?

- No..... 0
Yes..... 1
Refused to answer..... 7
Don't know..... 9

***If PA-1 in (0, 7, 9) AND participant injected in past 12 months, skip to PA-2.
Else, if PA-1 in (0, 7, 9) AND participant did NOT inject in past 12 months, skip to PA-4.***

***If PA-1=1 AND NHBS-MSM, go to PA-1a.
Else, if PA-1=1 AND NHBS-IDU, skip to PA-1b.
Else if PA-1=1 AND NHBS-HET, skip to PA-1c.***

PA-1a. ***[GIVE RESPONDENT FLASHCARD Q.]*** Which place or places on this list did you get free condoms from? ***[READ CHOICES. MARK ALL THAT APPLY.]***

- HIV/AIDS-focused community-based organization... 1
GLBTQ organization or community health center..... 2
Health center or clinic..... 3
Bar, club, bookstore, or other business..... 4
Some other place 5
Refused to answer..... 7
Don't know..... 9

Skip to PA-1d.

PA-1b. **[GIVE RESPONDENT FLASHCARD R.]** Which place or places on this list did you get free condoms from? **[READ CHOICES. MARK ALL THAT APPLY.]**

- HIV/AIDS-focused community-based organization... 1
- Needle or syringe exchange program..... 2
- IDU outreach program..... 3
- Health center or clinic..... 4
- Drug or alcohol treatment program..... 5
- Some other place 6
- Refused to answer..... 7
- Don't know..... 9

Skip to PA-1d.

PA-1c. **[GIVE RESPONDENT FLASHCARD S.]** Which place or places on this list did you get free condoms from? **[READ CHOICES. MARK ALL THAT APPLY.]**

- HIV/AIDS-focused community-based organization..... 1
- Health center or clinic..... 2
- Bar, club, bookstore, or other business..... 3
- Drug or alcohol treatment program..... 4
- Some other place..... 5
- Refused to answer..... 7
- Don't know..... 9

PA-1d. Have you used any of the free condoms you received?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

If injected drugs in past 12 months, go to PA-2. Otherwise, skip to PA-4.

PA-2. In the past 12 months, have you gotten any new sterile needles for free, not including those given to you by a friend, relative, or sex partner?

- No..... 0  *Skip to PA-3*
- Yes..... 1
- Refused to answer..... 7  *Skip to PA-3*
- Don't know..... 9

PA-2a. **[GIVE RESPONDENT FLASHCARD R.]** Which place or places on this list did you get the free sterile needles from? **[READ CHOICES. MARK ALL THAT APPLY.]**

- HIV/AIDS-focused community-based organization... 1
- Needle or syringe exchange program..... 2
- IDU outreach program..... 3
- Health center or clinic..... 4
- Drug or alcohol treatment program..... 5
- Some other place 6
- Refused to answer..... 7
- Don't know..... 9

PA-2b. Have you used any of the free sterile needles you received?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

PA-3. In the past 12 months, have you gotten any new cookers, cotton, or water for free, not including those given to you by a friend, relative, or sex partner?

- No..... 0  *Skip to PA-4*
- Yes..... 1
- Refused to answer..... 7  *Skip to PA-4*
- Don't know..... 9

PA-3a. **[GIVE RESPONDENT FLASHCARD R.]** Which place or places on this list did you get those free items from? **[READ CHOICES. MARK ALL THAT APPLY.]**

- HIV/AIDS-focused community-based organization... 1
- Needle or syringe exchange program..... 2
- IDU outreach program..... 3
- Health center or clinic..... 4
- Drug or alcohol treatment program..... 5
- Some other place 6
- Refused to answer..... 7
- Don't know..... 9

PA-3b. Have you used the free cookers, cotton, or water that you received?

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

PA-4. In the past 12 months, have you had a one-on-one conversation with an outreach worker, counselor, or prevention program worker about ways to prevent HIV? Don't count the times when you had a conversation as part of an HIV test.

- No..... 0  *Skip to PA-5*
- Yes..... 1
- Refused to answer..... 7  *Skip to PA-5*
- Don't know..... 9

If PA-4 in (0, 7, 9), skip to PA-5.

***If PA-4=1 AND NHBS-MSM, go to PA-4a.
Else, if PA-4=1 AND NHBS-IDU, skip to PA-4b.
Else if PA-4=1 AND NHBS-HET, skip to PA-4c.***

PA-4a. **[GIVE RESPONDENT FLASHCARD Q.]** Which type of organization did they work for?
[READ CHOICES. MARK ALL THAT APPLY.]

- HIV/AIDS-focused community-based organization... 1
- GLBTQ organization or community health center..... 2
- Health center or clinic..... 3
- Bar, club, bookstore, or other business..... 4
- Some other place 5
- Refused to answer..... 7
- Don't know..... 9

Skip to PA-4d.

PA-4b. **[GIVE RESPONDENT FLASHCARD R.]** Which type of organization did they work for?
[READ CHOICES. MARK ALL THAT APPLY.]

- HIV/AIDS-focused community-based organization... 1
- Needle or syringe exchange program..... 2
- IDU outreach program..... 3
- Health center or clinic..... 4
- Drug or alcohol treatment program..... 5
- Some other place 6
- Refused to answer..... 7
- Don't know..... 9

Skip to PA-4d.

PA-4c. **[GIVE RESPONDENT FLASHCARD S.]** Which type of organization did they work for?
[READ CHOICES. MARK ALL THAT APPLY.]

- HIV/AIDS-focused community-based organization... 1
- Needle or syringe exchange program..... 2
- IDU outreach program..... 3
- Health center or clinic..... 4
- Drug or alcohol treatment program..... 5
- Some other place 6
- Refused to answer..... 7
- Don't know..... 9

PA-4d. During those one-on-one conversation(s), did you: **[ASK EACH QUESTION, MARK NO OR YES FOR EACH]**

No Yes Refused to answer Don't Know

1. Discuss ways to talk to a partner about safe sex?.... 0... 1... 7..... 9

If yes, ask:

2. Practice ways to talk to a partner about safe sex?..... 0.... 1.... 7..... 9

3. Discuss ways to effectively use condoms?..... 0... 1... 7..... 9

If yes, ask:

4. Practice ways to effectively use condoms?..... 0... 1.... 7..... 9

[If injected drugs in past 12 months, ask:]

5. Discuss how to prepare for safe injections?..... 0... 1.... 7..... 9

If yes, ask:

6. Practice safe drug-injecting practices?..... 0... 1.... 7..... 9

PA-5. In the past 12 months have you been a participant in any organized session(s) involving a small group of people to discuss ways to prevent HIV? Don't include discussions you had with a group of friends.

- No..... 0
- Yes..... 1
- Refused to answer..... 7
- Don't know..... 9

If PA-5 in (0, 7, 9), skip to INT11.

If PA-5=1 AND NHBS-MSM, go to PA-5a.

Else, if PA-5=1 AND NHBS-IDU, skip to PA-5b.

Else if PA-5=1 AND NHBS-HET, skip to PA-5c.

PA-5a. **[GIVE RESPONDENT FLASHCARD Q.]** Which type of organization sponsored those sessions? **[READ CHOICES. MARK ALL THAT APPLY.]**

- HIV/AIDS-focused community-based organization... 1
- GLBTQ organization or community health center..... 2
- Health center or clinic..... 3
- Bar, club, bookstore, or other business..... 4
- Some other place 5
- Refused to answer..... 7
- Don't know..... 9

Skip to PA-5d.

PA-5b. **[GIVE RESPONDENT FLASHCARD R.]** Which type of organization sponsored those sessions? **[READ CHOICES. MARK ALL THAT APPLY.]**

- HIV/AIDS-focused community-based organization... 1
- Needle or syringe exchange program..... 2
- IDU outreach program..... 3
- Health center or clinic..... 4
- Drug or alcohol treatment program..... 5
- Some other place 6
- Refused to answer..... 7
- Don't know..... 9

Skip to PA-5d.

PA-5c. **[GIVE RESPONDENT FLASHCARD S.]** Which type of organization sponsored those sessions? **[READ CHOICES. MARK ALL THAT APPLY.]**

- HIV/AIDS-focused community-based organization... 1
- Needle or syringe exchange program..... 2
- IDU outreach program..... 3
- Health center or clinic..... 4
- Drug or alcohol treatment program..... 5
- Some other place 6
- Refused to answer..... 7
- Don't know..... 9

PA-5d. During those organized group session(s), did you: **[ASK EACH QUESTION, MARK NO OR YES FOR EACH.]**

- | | No | Yes | Refused to answer | Don't Know |
|--|-------------------------------|-------------------------------|---------------------------------|----------------------------|
| 1. Discuss ways to talk to a partner about safe sex?.... | <input type="checkbox"/> 0... | <input type="checkbox"/> 1... | <input type="checkbox"/> 7..... | <input type="checkbox"/> 9 |
| <i>If yes, ask:</i> | | | | |
| 2. Practice ways to talk to a partner about safe sex?..... | <input type="checkbox"/> 0... | <input type="checkbox"/> 1... | <input type="checkbox"/> 7..... | <input type="checkbox"/> 9 |
| 3. Discuss ways to effectively use condoms?..... | <input type="checkbox"/> 0... | <input type="checkbox"/> 1... | <input type="checkbox"/> 7..... | <input type="checkbox"/> 9 |
| <i>If yes, ask:</i> | | | | |
| 4. Practice ways to effectively use condoms?..... | <input type="checkbox"/> 0... | <input type="checkbox"/> 1... | <input type="checkbox"/> 7..... | <input type="checkbox"/> 9 |
| <i>[If injected drugs in past 12 months, ask:]</i> | | | | |
| 5. Discuss how to prepare for safe injections?..... | <input type="checkbox"/> 0... | <input type="checkbox"/> 1... | <input type="checkbox"/> 7..... | <input type="checkbox"/> 9 |
| <i>If yes, ask:</i> | | | | |
| 6. Practice safe drug-injecting practices?..... | <input type="checkbox"/> 0... | <input type="checkbox"/> 1... | <input type="checkbox"/> 7..... | <input type="checkbox"/> 9 |

BEFORE BEGINNING THE LOCAL QUESTIONS, THE INTERVIEWER ANSWERS THE FOLLOWING QUESTION. DO NOT READ THIS QUESTION TO THE RESPONDENT.

INT11. How confident are you of the validity of the respondent's answers?

Confident..... 1

Some doubts..... 2

Not confident at all..... 3

If response is 2 or 3, please explain why you are not confident in the respondent's answers:

Auto8. Time core questionnaire ended: __ __: __ __ 1 AM 2 PM

INTERVIEWER INSTRUCTIONS:

Please confirm. Did the person complete the survey?

- No (did not complete the survey).....* *0*
Yes (did complete the survey)..... *1*

If consent for HIV test not recorded (CN-2 = 0), go to CONF23.

CONF23. INTERVIEWER INSTRUCTIONS:

SAY: My records reflect that you did not agree to HIV testing when asked earlier during the interview. Before I close out the survey, I'd like to ask you again about whether or not you would like an HIV test. Did you want the HIV test that is part of today's survey?

- Yes (respondent DOES want the test).....* *1*
No (respondent DOES NOT want the test)..... *0*

If CONF23 =1, go to INT12.

INT12. Interviewer Instructions:

Indicate each activity the participant consents to. CHECK ALL THAT APPLY

- HIV testing and counseling*
- Having other lab tests (if offered)*
- Storing a blood specimen for future testing*

FOR NHBS-IDU

Message about Eligibility to Receive Coupons:

If COMPLETE=1 AND VALIDITY ≠ 3:

"This respondent is ELIGIBLE to recruit others and receive coupons."

Message about not being eligible to receive coupons:

If VALIDITY = 3 OR COMPLETE=0:

"This respondent is NOT eligible to recruit others or receive coupons."

LOCAL USE QUESTIONS FOLLOW

After completing the local questions say:

Do you have any questions about the issues we've talked about?

Thank the respondent for their time and end the interview.

National HIV Behavioral Surveillance System: Flashcards

FLASHCARD A

- American Indian or Alaska Native
- Asian
- Black or African American
- Native Hawaiian or Other Pacific Islander
- White

FLASHCARD B.1

- A relative or family member
- A person you have sex with
- A person you use drugs with or buy drugs from
- A friend
- An acquaintance
- A stranger

FLASHCARD B.2

- A relative or family member
- A person you have sex with
- A friend
- An acquaintance
- A stranger

FLASHCARD C

How many people do you know who are:

- Friends, relatives, or other people you are close to, AND
- Who are at least 18 years old, AND
- Who live in *[insert project area]*

FLASHCARD D

- Married
- Living together as married
- Separated
- Divorced
- Widowed
- Never married

FLASHCARD E

	<u>MONTHLY INCOME</u>	<i>OR</i>		<u>YEARLY INCOME</u>
A.	\$0 to \$417		A.	\$0 to \$4,999
B.	\$418 to \$833		B.	\$5,000 to \$9,999
C.	\$834 to \$1,041		C.	\$10,000 to \$12,499
D.	\$1,042 to \$1,250		D.	\$12,500 to \$14,999
E.	\$1,251 to \$1,667		E.	\$15,000 to \$19,999
F.	\$1,668 to \$2,082		F.	\$20,000 to \$24,999
G.	\$2,083 to \$2,500		G.	\$25,000 to \$29,999
H.	\$2,501 to \$2,916		H.	\$30,000 to \$34,999
I.	\$2,917 to \$3,333		I.	\$35,000 to \$39,999
J.	\$3,334 to \$4,167		J.	\$40,000 to \$49,999
K.	\$4,168 to \$4,999		K.	\$50,000 to \$59,999
L.	\$5,000 to \$6,250		L.	\$60,000 to \$74,999
M.	\$6,251 or more		M.	\$75,000 or more

FLASHCARD F

Insurance Coverage

- Private health plan
- Medicaid / *[insert local Medicaid name]*
- Medicare
- Other Medical Assistance program *[insert local Non-Medicaid public health plan name]*
- TRICARE (CHAMPUS)
- Veterans Administration coverage
- Some other health care plan

FLASHCARD G

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly disagree

FLASHCARD H.1

Definition of "Having Sex"

Oral, vaginal, or anal sex.

- Oral sex means mouth on the vagina or penis
- Vaginal sex means penis in the vagina
- Anal sex means penis in the anus (butt)

FLASHCARD H.2

Definition of "Having Sex"

Oral or anal sex.

- Oral sex means mouth on the penis
- Anal sex means penis in the anus (butt)

FLASHCARD I

Female Sex Partners

Main partner:

A woman you have sex with and who you feel committed to above anyone else. This is a partner you would call your girlfriend, wife, significant other, or life partner.

Casual partner:

A woman you have sex with but do not feel committed to or don't know very well.

FLASHCARD J

Male Sex Partners

Main partner:

A man you have sex with and who you feel committed to above anyone else. This is a partner you would call your boyfriend, husband, significant other, or life partner.

Casual partner:

A man you have sex with but do not feel committed to or don't know very well.

FLASHCARD K

0. Never
1. More than once a day
2. Once a day
3. More than once a week
4. Once a week
5. More than once a month
6. Once a month
7. Less than once a month

FLASHCARD L
FOR USE WITH ALCOHOL QUESTIONS



1 Shot of Liquor
(Whisky, Vodka, Gin, etc.)
1.5 oz.



1 Regular Beer
12 oz.



1 Glass of Wine
5 oz.

FLASHCARD M

- a. Pharmacy or drug store
- b. Doctor's office, clinic, or hospital
- c. Friend, acquaintance, relative, or sex partner
- d. Needle or drug dealer, shooting gallery, hit house, off the street
- e. Needle exchange program

FLASHCARD N

- 0. Never
- 1. Rarely
- 2. About half the time
- 3. Most of the time
- 4. Always

FLASHCARD O

0. Sex partner
1. Friend or acquaintance
2. Relative
3. Needle or drug dealer
4. Stranger

FLASHCARD P

- Doctor or other health care provider
- Sex partner, friend, relative, or acquaintance
- Internet
- Some other place

FLASHCARD Q

- HIV/AIDS-focused community-based organization
- GLBTQ organization or community health center
- Health center or clinic
- Bar, club, bookstore, or other business
- Some other place

FLASHCARD R

- HIV/AIDS-focused community-based organization
- Needle or syringe exchange program
- IDU outreach program
- Health center or clinic
- Drug or alcohol treatment program
- Some other place

FLASHCARD S

- HIV/AIDS-focused community-based organization
- Health center or clinic
- Bar, club, bookstore, or other business
- Drug or alcohol treatment program
- Some other place

English Version; Grade Reading Level by Flesch-Kincaid Method: 7.6

National HIV Behavioral Surveillance System Model Consent Form

The [Agency Name] and the Centers for Disease Control and Prevention (CDC) invite you to be part of a research study of persons who may be at risk for HIV infection. The information I will give you can help you make a good choice about joining the study.

A. Why we are doing this project

The purpose of this study is to learn about risk for HIV. We will use this information to plan better HIV prevention and treatment programs for people in your community. Being in this study is voluntary.

B. What will happen

If you agree to be in this study, this is what will happen.

1. You will do a survey with a trained staff member.

The survey has questions about your health, drug use, sex practices, and HIV prevention services. It will take about 40 minutes.

2. If you agree to the survey, we will offer you a free HIV test. If you already know that you are HIV-infected, we would still like to offer you an HIV test today so that we can link today's HIV test result with your survey results.
3. *[For sites doing HIV tests via blood draw only]* If you agree to an HIV test, you will also be asked to have your blood sample stored
4. *[For sites doing additional lab tests]* If you agree to the HIV test, we will also offer you free *[other lab tests]*

This is an anonymous survey. We will not ask for your name or other identifying information. The survey has questions that are personal. They may be hard to talk about. You may refuse to answer any questions at any time for any reason. If you refuse to answer a question or want to end the interview you will not be punished in any way.

If you agree to the HIV test, you will have a 10- to 15-minute HIV prevention counseling session with a trained staff member. The session will cover the meaning of results from the HIV test. You will also learn about how to reduce your chances of being infected with HIV and other infectious diseases. You may still take the survey and HIV test even if you already know your HIV status.

The HIV test will be done by a standard or rapid test as discussed below.

Standard Test

For the standard test, we will [draw less than 1 tablespoon of your blood using a needle/swab the inside of your mouth for oral fluid] and test it for HIV. Your test results will be ready within one week. We will set up a day and time for you to get your results. You will get counseling about what the test results mean and referrals to services, if needed. *[For sites that allow HIV test phone results: If you cannot return for your HIV test results, you can arrange to receive your counseling and test results by telephone.]*

Rapid Test

With the rapid test, you can get the result of your HIV test within 1 hour. We will [stick the tip of one of your fingers to obtain a few drops of blood/take a swab from your mouth]. You will get counseling about what the test result means. You will get referrals to services, if needed. If the rapid test result is reactive, or if you know you are already HIV- infected, we will [draw less than 1 tablespoon of your blood by needle/stick the tip of one of your fingers to obtain a few drops of blood/swab the inside of your mouth for oral fluid] for a second test to confirm your rapid test result. The result of the confirmatory test will be ready within one week. We will set up a day and time for you to get your results.

Rapid Test Algorithm

With the rapid test, you can get the result of your HIV test within 1 hour. We will [stick the tip of one of your fingers to obtain a few drops of blood/take a swab from your mouth]. You will get counseling about what the test result means. If the first rapid test is reactive, or if you know you are already HIV- infected, we will do up to two additional tests to confirm your results. For the additional rapid tests, we will [draw less than 1 tablespoon of your blood by needle/stick the tip of one of your fingers to obtain a few drops of blood/swab the inside of your mouth for oral fluid]. Finally, we will use this same [blood/oral fluid] to confirm your rapid test result in a laboratory. The result of the confirmatory test will be ready within one week. We will set up a day and time for you to get your results.

Linkage

We will link your test results with your survey so we can learn about sexual and drug-use risk behaviors known to be connected with HIV infection. We will link your test results using the same ID assigned to the survey. This is an anonymous test. Your name will not be on the test results or the survey. No one besides you will be told your test results, and neither the survey nor the test will be placed in any medical record.

We would like to store any blood that is left over after we do your test. We plan to use this sample for studies we will do in the future. We will store your sample with some data about you, such as your age, race, and sex. We will not put your name on the sample and there will be no way to know it is yours: thus, we will not be able to report back any test results to you. We will not test for any genetic disease or use blood for cloning or commercial purposes. You can decline to let us store your blood and still be in this study. Your blood sample will be destroyed after this testing is completed.

[Hepatitis B, Hepatitis C].

[Include any additional test to be offered].

C. Things to consider

There are minimal risks from being in this study:

1. Some of the questions in the survey are about sex and drugs and may make you feel uncomfortable. All answers you give will be kept private.
2. [*If using standard test:* Drawing blood may cause temporary discomfort from the needle stick, bruising, bleeding, light-headedness, and local infection.]
3. You may feel uncomfortable finding out you might have been infected with HIV. You can talk about your concerns with the trained staff member who tells you your HIV test results, if you wish.
4. If your HIV test result is negative, there is a slight chance that the results are wrong and that you could still be infected or test positive at some time in the future.

D. Benefits

Benefits you may get from being in this study include:

1. You will receive some condoms and information on HIV/AIDS and STDs.
2. You will, if you wish, receive free referrals to other local programs, medical programs, support groups, and health projects, as needed.
3. If your HIV test results [*or additional tests offered*] are positive, you will be counseled about ways to prevent the spread of infection. You will also be referred for medical care.
4. If your test results are negative, you will receive counseling on how to prevent future infections.

Also, information gained from this study will help the [Agency Name] to know more about HIV and how it is spread. This information will be used to improve health programs and to develop new ways of helping others prevent disease and promote good health.

E. Alternatives

If you choose not to take part in the study but would like to take an HIV test, we will inform you of agencies or organizations that provide testing. You will get no medical treatment in this study.

F. Compensation

You will be paid for the time you spend taking part in the study. For completion of the survey, you will get \$25. If you take part in the HIV test, you will get an additional \$25.

G. Persons to Contact

This study is run by: *[name of principal investigator and phone number]*. You may call [him/her] with any questions about being in the study.

If you have questions about your rights as a participant or if you feel that you have been harmed, contact *[IRB committee or contact name and phone number]*.

If you want one, you will get a copy of this form to keep.

H. Confidentiality Statement

What you tell us is confidential. Your responses will be labeled with a study number only. No one except the study staff at **[Agency Name]** and CDC will have access to the survey, except as otherwise required by law. Your responses will be grouped with survey answers from other persons.

Survey forms and handheld computers will be locked in a file cabinet at the study office. Computers with study data will be physically secured and protected by coded passwords. Only specific study staff will have access to the locked file cabinet or the computers.

If you know me, you may ask for another staff member so that your answers will be fully private.

I. Costs

You will not be charged for counseling, the HIV test *[any additional tests offered]*, safer sex and HIV prevention materials, referrals to appropriate agencies, or any other services provided by this study.

J. Right to Refuse or Withdraw

This study is completely VOLUNTARY. You are not giving up any legal claims or rights for being a part of this study. If you agree to participate, you are free to quit at any time. You can choose to only do the survey and not to have an HIV test.

K. Agreement

Do you have any questions?

Interviewer: Answer the participant's questions before proceeding to the next question.

You have read or had read to you the explanation of this study, you have been given a copy of this form, the opportunity to discuss any questions that you might have and the right to refuse participation. I am going to ask for your consent to participate in this study.

(Consent will be documented by the interviewer in the handheld computer as follows:)

Do you agree to take part in the survey?

- Yes
- No

Do you agree to HIV counseling and testing?

- Yes
- No

Do you agree to having other lab tests (if offered)?

- Yes
- No

Do you agree to storing a blood sample for future testing (if offered)?

- Yes
- No

If survey declined:

We're interested in knowing why people do not want to do this study. Would you mind telling me which of the following best describes the reason you do not want to do this study?

- You don't have time..... 1
- You don't want to talk about these topics..... 2
- Some other reason, or 3
- You'd rather not say why..... 9

Appendix G

Improved Referral to Care for NHBS-MSM3 Participants using a Rapid Test Algorithm

Overview

In recent years, the development and validation of point-of-contact (POC) rapid testing algorithms (RTA) using multiple rapid tests has become an important initiative. These algorithms would allow persons to receive a corroborated HIV test result on-site while they wait. Individuals found to be HIV-positive could then be immediately referred into care in that same visit. The development and validation of these HIV rapid testing algorithms is supported by projects such as CDC protocol #5165 entitled, “Evaluation of a Rapid HIV Test Algorithm for Improved Predictive Value and Improved Linkage to Care”. Protocol #5165 sought to evaluate the performance of a RTA relative to Enzyme Immunoassay (EIA)/Western blot (WB) and demonstrated the feasibility of implementing such an algorithm in US HIV counseling and testing sites serving high risk clients.

This RTA protocol for NHBS-MSM3 addresses an interest on the part of some NHBS investigators to refer HIV-infected men into care more quickly than is possible with standard laboratory-based testing. Performing multiple tests will allow for immediate referral of clients reactive on two or more tests, depending on the RTA used, although persons with discordant rapid test results may be referred for additional testing. The prevalence of HIV among MSM in 21 NHBS cities was 19% (range: 6% - 38%)¹ therefore, most NHBS-MSM3 participants tested will have a non-reactive initial rapid test result and will not require further testing. However, the rapid test algorithm would preferably begin with the most sensitive test, one using blood as opposed to oral fluid, so that early stage infections are not missed by the first rapid test.

The NHBS-MSM3 RTA is optional for project sites and is based on methods used in CDC protocol #5165 mentioned above. In order to implement a rapid testing algorithm, NHBS project sites must be able to:

- Perform rapid HIV testing
- Collect a sample (oral or blood) for laboratory-based confirmatory testing
- Schedule an appointment to return the result of laboratory-based confirmatory testing
- Train testers for using rapid HIV tests included in the testing algorithm
- Provide quality assurance for all rapid HIV tests included in the rapid testing algorithm

Background

With the availability of FDA-approved HIV rapid screening tests that are both highly sensitive and specific, alternative algorithms that use multiple rapid point of care tests rather than relying

on laboratory-based Western blot (WB) confirmation are being considered. Rapid, point-of care HIV screening tests have gained popularity because results from the initial HIV screen can be determined in as little as 20 minutes and can be performed by non-Clinical Laboratory Improvement Amendments (CLIA) certified technicians in a variety of settings. However, the confirmatory WB can take one to two weeks before results can be reported. With rapid testing, nearly all clients receive the results of their initial rapid test, but many who test preliminary positive fail to return for their confirmatory results. In a review of client-level rapid HIV testing data in October of 2005, the California State Office of AIDS noted that only 48% of preliminary positive rapid tests in the State had a documented disclosure of the confirmed HIV test result over the last year.²

A rapid HIV testing algorithm that eliminates the need for off-site confirmatory testing and a return visit for results prior to referral to care would help ensure that those individuals with greatest need for direct linkage to care and other services could be referred at the earliest possible moment. The algorithm would also eliminate the number of false positive rapid HIV screening test results reported to clients. Uninfected clients who receive these false positive rapid test results currently have to wait until the results of laboratory confirmation are available before learning that they are uninfected. Adding a second and third rapid test performed at the point of care would provide more information to both client and counselor, by improving the likelihood that someone with reactive results from two different tests is actually infected, and identifying likely false positive screening tests if the second and third tests are both non-reactive.

In 1994 UNAIDS and WHO recommended the use of three different testing strategies using multiple simple rapid tests in resource limited settings without a confirmatory Western blot or Indirect Immunofluorescent Assay (IFA).³ This decision was based upon evidence from studies showing that the “combinations of EIA and/ or simple/ rapid assays can provide results as reliable as, and in some instances more reliable than, the EIA/ Western blot combination, and at a much lower cost.” Several studies in developing countries have shown the reliability of using multiple simple/rapid tests as an HIV testing algorithm instead of the traditional laboratory-based EIA/Western blot HIV testing algorithm.⁴⁻⁶

There are several RTAs being considered for use in the U.S.⁷ To date, no RTA has been widely accepted and written into official guidelines; therefore, confirmatory testing with laboratory-based tests is required to diagnose individuals with reactive rapid test results. It is important to note that a rapid test algorithm is only as sensitive as the first test used, and that persons may receive a false-negative screening test result if a rapid test is used that is not sensitive for early infection. This may particularly be an issue in a population with a high proportion of new infections.

Algorithm Descriptions

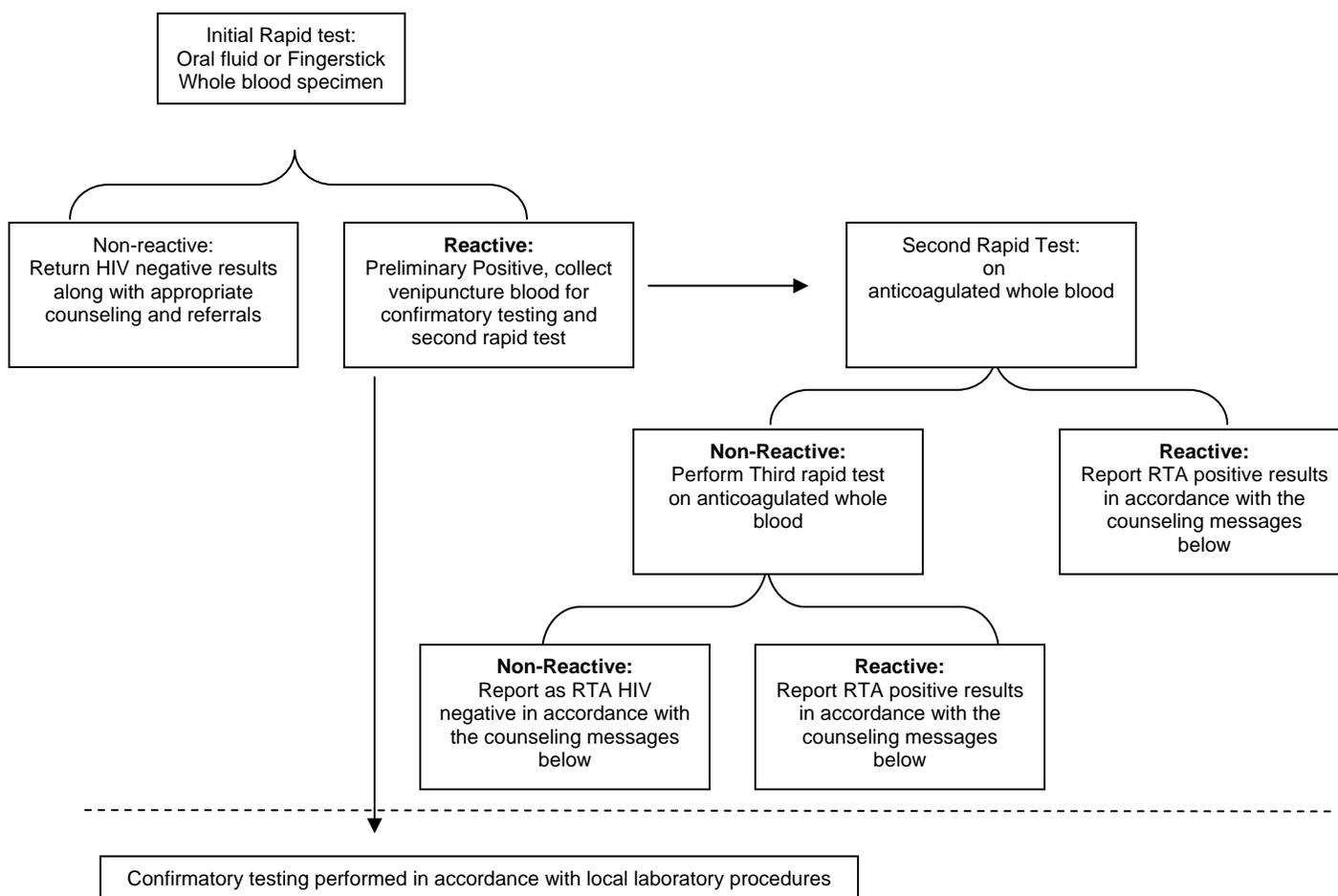
NHBS-MSM3 project sites can choose from one of two algorithms:

Rapid Testing Algorithm (RTA) – Phlebotomy required

Figure 2A illustrates a serial rapid HIV testing algorithm for potential use at NHBS-MSM3 RTA sites. If the first rapid test is reactive, blood (EDTA plasma in a “purple top” tube) will be drawn for laboratory-based testing in accordance with local procedures for confirmation of a preliminary positive rapid test and this anticoagulated whole blood sample will be used to perform a second rapid test. If this second rapid test is also reactive the client will be given the results of the rapid tests as described below and referred to care. If the second test is negative, the anticoagulated whole blood collected for confirmatory testing will again be accessed to perform a third rapid test. The tests used in the algorithm must be from a different manufacturer. The participant will then receive post test counseling based on the result of this third test as described below, and, if reactive, will be referred for follow-up care.

Supplemental testing will be performed by the laboratory currently used for local laboratory-based HIV confirmatory testing on whole blood specimens.

Figure 1. Serial Rapid Testing Algorithm requiring phlebotomy

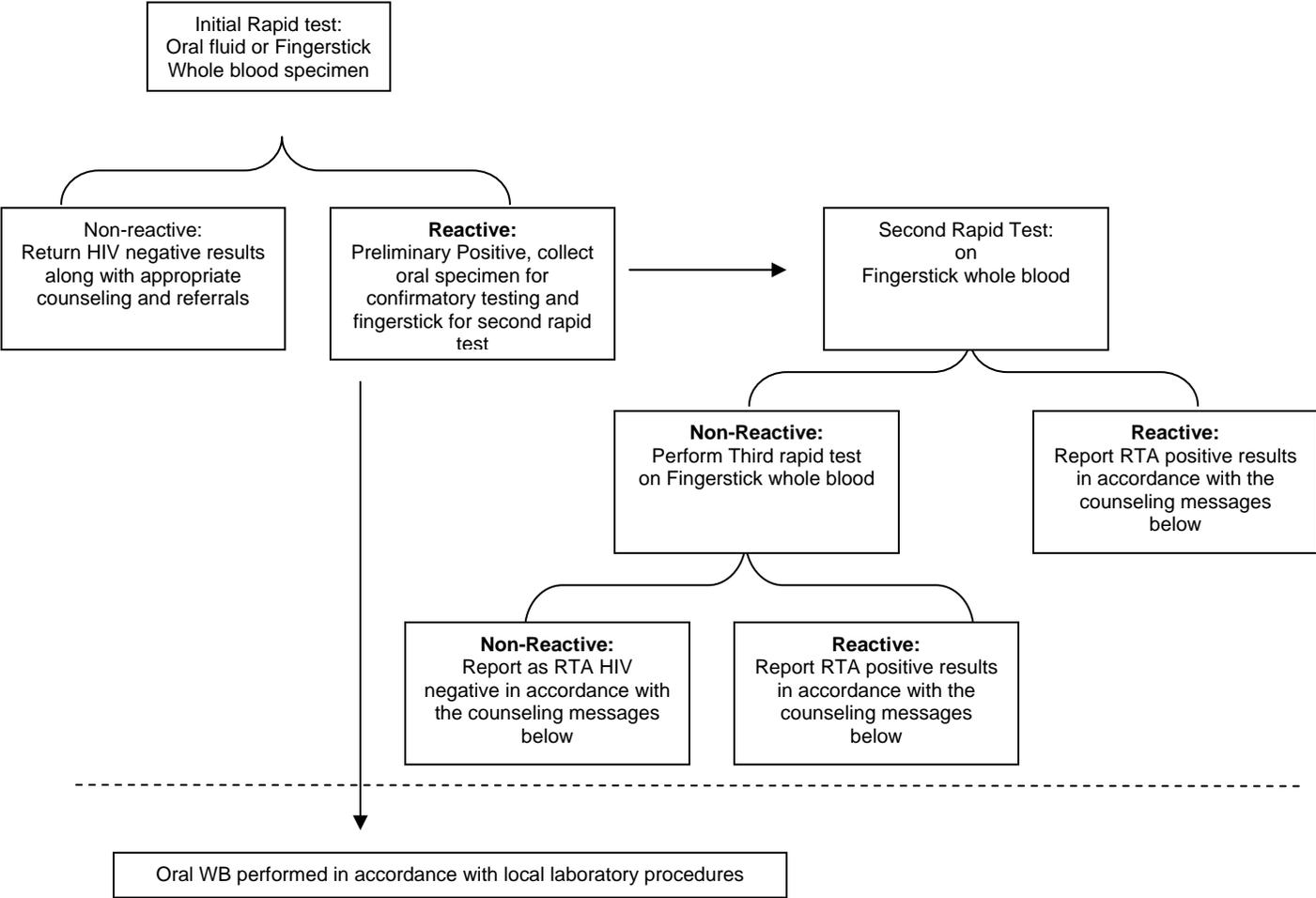


Rapid Testing Algorithm (RTA) – Phlebotomy NOT required

Figure 3 illustrates another serial rapid HIV testing algorithm for potential use at a NHBS-MSM3 RTA sites. If the first rapid test is reactive, an OraSure OMT specimen will be collected for laboratory-based testing in accordance with local procedures for confirmation of a preliminary positive rapid test and a fingerstick sample will be used to perform the second rapid test. If this second rapid test is also reactive the client will be given the results of the rapid tests as described below and referred to care. If the second test is negative, another fingerstick sample will be obtained to perform a third rapid test. The tests used in the algorithm must be from a different manufacturer. The participant will then receive post test counseling based on the result of this third test as described below, and, if reactive, will be referred for follow-up care.

A Supplemental WB will be performed by the laboratory currently used for local laboratory-based HIV confirmatory testing on oral specimens.

Figure 2. Serial Rapid Testing Algorithm not requiring phlebotomy



Counseling Messages

NHBS-MSM3 participants will receive results of all rapid tests performed at the time they are tested. Counseling will be provided to participants based on the following combinations of rapid test results:

Initial (Screening) rapid test non-reactive: Participants will be counseled in accordance with local and federal guidelines for counseling of persons who test HIV negative.

Initial (Screening) rapid test reactive, second and third rapid test non-reactive: Participants who screen rapid test reactive but then have two subsequent rapid tests that are non-reactive will be informed that based on their non-reactive rapid test results, the first reactive test was most likely false positive. These participants will be told that additional laboratory testing will be performed on the blood or oral specimen that was collected, but that it is expected that the results of the laboratory testing will indicate the participant is not infected. Participants will receive counseling based on identified risks for HIV infection. Participants may obtain their laboratory results in accordance with local procedures established for NHBS-MSM3.

Initial (Screening) rapid test reactive, second or third rapid test reactive: Participants who have two reactive rapid HIV tests will be counseled in accordance with local and federal guidelines for counseling persons who have reactive rapid HIV test results, and that based on the two concordant reactive rapid test results, it is likely that they are infected with HIV. Participants will be referred to HIV medical care using the local procedures established for NHBS-MSM3. These participants will be told that laboratory testing will be performed on the blood or oral specimen that was collected, and that it is expected that the results of the laboratory testing will indicate the client is HIV infected. Participants will receive appropriate counseling based on identified risks for HIV infection. Participants may obtain their laboratory results in accordance with the local procedures established for NHBS-MSM3.

Informed Consent

Participants will be consented in accordance with the NHBS-MSM3 protocol. Project sites may need to add language to their local consent form to describe the additional testing process following an initial reactive rapid test. Any changes made to the NHBS-MSM3 model consent form for the purposes of implementing the RTA will be sent to CDC Project Officer for review and approval.

As with standard NHBS-MSM3 testing procedures, all tests done for the RTA will be anonymous.

Training

NHBS project sites are responsible for the training or certification of staff in specimen collection and rapid test performance and adhering to quality assurance guidelines for rapid testing. CDC NHBS staff will provide technical assistance to describe the study, provide specific instructions for providing counseling messages associated with the results of the RTA, and describe the process of performing multiple rapid tests.

Data Collection

RTA data will be collected in accordance with the usual NHBS-MSM3 procedures. HIV testing logs will need to be amended to include test results from multiple rapid tests. Each site using the RTA must have the HIV testing log approved by a CDC Project Officer before the RTA can be implemented.

References

1. CDC. Prevalence and Awareness of HIV Infection among Men Who Have Sex with Men – 21 Cities, United States, 2008. *Morbidity and Mortality Weekly Report* 59(37), 1201-1207. 9-24-2010.
2. Sykes D. OraQuick Advance: Delivering Results. 2005.
3. Sato PA, Maskill WJ, Tamashiro H, Heymann DL. Strategies for laboratory HIV testing: an examination of alternative approaches not requiring Western blot. *Bulletin of the World Health Organization* 1994;72(1):129-34.
4. Granade TC. Use of rapid HIV antibody testing for controlling the HIV pandemic. *Expert review of anti-infective therapy* 2005 December;3(6):957-69.
5. Granade T, Phillips S, Parekh B et al. Detection of antibodies to human immunodeficiency virus type 1 in oral fluids: a large-scale evaluation of immunoassay performance. *Clin Diagn Lab Immunol* 5, 171-175. 1998.
6. Stetler HC, Granade TC, Nunez CA et al. Field evaluation of rapid HIV serologic tests for screening and confirming HIV-1 infection in Honduras. *AIDS* 1997 March;11(3):369-75.
7. Association of Public Health Laboratories and the Centers for Disease Control & Prevention. HIV testing algorithms — A status report. [cited 2010 August 27]; Available from: <http://www.aphl.org/aphlprograms/infectious/hiv/Documents/StatusReportFINAL.pdf>
8. Centers for Disease Control and Prevention. Notice to Readers: Protocols for Confirmation of Reactive Rapid HIV Tests. *MMWR*. 2004; 53 (10): 221-222.

Appendix H

Model HIV Phone Result Protocol

Note: This protocol was used by Los Angeles County staff for Project 1 (IRB#3901).

Goal: To provide telephone HIV results and posttest counseling to eligible clients in a confidential, sensitive, and safe manner while meeting mandated requirements for counseling HIV-positive persons.

I. Eligibility criteria

- A. During pre-test sessions, all clients will be offered the option of receiving test results either by a phone call, or by an in-person appointment. The option is to be offered to the client in a neutral tone, with no attempt made to influence the client's decision about which option to choose.
- B. Clients must agree to meet in person with one of the study counselors or a health care provider within 48 hours after a positive or indeterminate result is given.
- C. Clients must have the UTC code, lab slip number, and a unique "password" available when the call is made to get results.
- D. Clients should identify at least one person in their support system that they could talk to if the test is positive or indeterminate.

II. Procedure

- A. Clients who meet the eligibility criteria for phone results will be asked if they want to receive results over the phone. The Phone Result phone number is_____.
 1. Clients may choose to return in person for their results.
 2. Counselors may deny phone results to eligible clients if their mental status, i.e., anxiety, depression, or the need for structured posttest counseling indicates a need to return in person for results.
 3. Consult [**Supervisor's name**] if you have questions about eligibility for phone results.
- B. Study counselors
 1. Clients will be asked to identify one support person and a unique "password" (such as their mother's birthdate or the last 4 digits of a social security number).
 2. Clients will be given a phone result card with the phone result line number, the client's UTC code, lab slip number, and specific times to *call for results*. **Inform the client that she/he must remember her/his password**—without it, he will have to return to the testing site to get results.
 3. Calls for phone results will be taken on Mondays, Wednesdays, and Fridays, between the hours of 10:00 AM - 12:00 PM and 2:00 PM - 4:00 PM. Voice mail will be activated during other times.
 4. Clients must provide the UTC code, lab slip number, and password *before HIV test results and posttest counseling will be given by phone*. Clients without this information need to return for results in person. Clients who call the phone result

number outside of scheduled hours will be transferred to the phone result voice mail or be asked to call back during phone result hours.

5. If a test result is *positive or indeterminate*, study counselors will speak with the client on the phone, assure that the client is not immediately suicidal, and arrange a time within the next 48 hours to: 1) meet in person with the client or; 2) arrange for an appointment with follow-up HIV care and treatment. The meeting can be at the project's mobile clinic van, at health care provider's office, or at a place the client chooses. At that time risk reduction counseling, emotional support, partner notification, and referral to the community referrals will be made.
 6. Clients with *positive or indeterminate* test results will be contacted by phone if they have not received their result in 7 days after their initial phone result was scheduled (provided that they left a phone number during the pre-test counseling session for this purpose).
 7. Study counselors will not leave test results on the client's answering machines or voice mail.
 8. Clients' UTC code, lab slip number, and password will be written in the phone appointment book and kept in a locked cabinet.
- C. Paperwork
1. Pre-test
 - a) Document client eligibility criteria, password, and additional instructions in testing chart.
 - b) Complete information on Phone Result Card.
 - c) Assure that UTC, lab slip number, and password are written in the phone appointment book.
 2. Posttest
 - a) Check "phone" in the "appointment type" section of the regular testing log book.
 - b) Enter date that test result is given in both the phone appointment book and regular testing log book.
 - c) Document posttest counseling. In a client with a positive or indeterminate result, the plan for social support, information about suicide intent, and follow-up meeting date and time must be written in the chart notes and phone appointment book.
 - d) Handling an upset, tearful, angry client or a client threatening suicide.
 - (1) Client threatening suicide.
 - (a) **Be calm, take slow deep breaths, keep client engaged in conversation.**
 - (b) Get help---supervisor or another counselor.
 - (c) If client is alone and has means and intention for suicide, ask someone to call the Cedars-Sinai Psychological Trauma Center @ 310-423-3506. This team will go to the location of the suicidal client and provide services. Stay on the phone with the client until help arrives.
 - (2) Upset, tearful, or angry client.

- (a) **Be calm, take slow deep breaths, listen, validate feelings.**
- (b) Use active listening.
- (c) Ask if there is a friend you can call to come be with client.
- (d) Stay with client on phone until the client doing better. Problem solve what to do now. Make arrangements to meet with the client the next day.
- (e) Refer to therapist or support group.

D. Other

- 1. Any calls for phone results during non-disclosure times should be transferred to the phone result voice mail or asked to call back during the voice mail times.
- 2. Voice mail message
 - a) Hello, you have reached 213-351-8173. Staff is available from 10:00 AM to 12:00 noon, and 2:00 PM and 4:00 PM on Mondays, Wednesdays, and Fridays to give results. If you have a question or want a result, please call back during these times. If you reach a busy signal during these times you may leave a message or call back in several minutes.

E. Evaluation

- 1. The Phone Results Protocol will continue for three months before an assessment of its effectiveness is conducted.
- 2. Data examined will be the number of clients who returned for their results and the number of HIV positives, comparing to three months prior to initiation of Phone Results Protocol.
- 3. Ask clients what they think of phone results and was this service helpful.
- 4. Keep a log or problems and difficult situations encountered. Report any adverse events to the supervisor immediately.
- 5. Conduct a weekly debriefing session of phone results; develop strategies to deal with problems.

Memorandum
Department of Health and Human Services
Public Health Service
Food and Drug Administration
Center for Biologics Evaluation and Research

TELEPHONE RECORD

Dates of Conversation: March 4 & March 15, 2005

Subject: Continued use of CDC/Calypte BED HIV Assay

Sponsor/Product: Centers for Disease Control
Human Immunodeficiency Virus Type 1 (HIV-1) (Murine Monoclonal Antibody) Antigen Detection EIA (Abbott) (Desensitized by CDC)

Prepared By: Michael Wiack, Regulatory Project Manager, CBER/OBRR/DBA

Date Prepared: April 27, 2005 

FDA Attendees:
Martin Ruta (March 4)
Kimberly Cressotti (March 4 & 15)
Michael Wiack (March 4)

Sponsor Attendees:
Bernard Branson (CDC)
George Richard (Calypte)
Don Kafader (Calypte)

FDA requested this telecon to discuss labeling questions regarding the Calypte "Incidence" test raised by Calypte and CDC and to discuss the use of this assay in the US. Both CDC and Calypte gave permission to FDA to speak to both parties about the study and use of the Calypte assay.

Calypte has licensed the manufacture of the HIV incidence test kit that CDC developed. CDC will maintain control of the distribution and use of this test kit within the US. Calypte plans on marketing this test kit outside the US without restrictions by CDC.

In the US, the test will be used only for surveillance purposes under CDC protocols. It will not be used for patient management or diagnosis and the test results will not be provided to the patient or physician. Neither an IDE nor an IND would be required for this use.

CDC/Calypte BED HIV Assay

CDC had requested labeling other than "RUO" labeling for use on the kits to be used within the United States, FDA would allow labeling "Not for diagnostic or clinical use. For surveillance use only." FDA did not otherwise review the labeling. Both CDC and Calypte agreed to this change for kits used within the US.

CDC asked about use of the test for patient management. FDA said such use would require an IDE. FDA should be contacted about IDE requirements, if either CDC or Calypte decides to pursue use of the test for diagnostic purposes including patient management.

Kimberly Cressotti spoke with CDC and Calypte regarding export of this device for the same intended use as stipulated for use and distribution in the US. Use of the label "Not for diagnostic or clinical use. For surveillance use only." is appropriate for exporting this device if it is for the same intended use as stipulated for use in the US. However, if Calypte wants to market the test kit for diagnostic purposes outside the US, Calypte will need to contact me to discuss labeling requirements.

Appendix J

Model HIV Testing Log

Log for Rapid HIV Testing Project Areas:

Rapid HIV Test Results Log										
Survey ID	Lab ID	Rapid Test Method	Self-reported HIV+ during interview? (Y/N)	Rapid Test Result	Returned Rapid Test Result (Y/N)	<i>For preliminary HIV+:</i> Collected Confirmatory Specimen (Y/N)	<i>For preliminary HIV+:</i> Type of Confirmatory Specimen	<i>For preliminary HIV+ if did not self-report HIV+ during interview:</i> Self-reported HIV+ during counseling session? (Y/N)	<i>For preliminary HIV+ if did not self-report HIV+ during counseling:</i> Likelihood participant knew they were HIV+ (Likely, Unsure, Unlikely)	Comments*

* If unable to collect a confirmatory specimen, provide reason in comments section.

Log for Standard HIV Testing Project Areas:

Standard HIV Test Results Log							
Survey ID	Lab ID	Collected Lab Specimen (Y/N)	Specimen Type	Self-reported HIV+ during interview? (Y/N)	<i>If did not self-report HIV+ during interview:</i> Self-reported HIV+ during counseling session? (Y/N)	<i>For those with HIV+ results who returned for their results:</i> Likelihood participant knew they were HIV+ (Likely, Unsure, Unlikely)	Comments*

* If unable to collect a confirmatory specimen, provide reason in comments section.

Appendix K

Assurance of Confidentiality for HIV/AIDS Surveillance Data

ASSURANCE OF CONFIDENTIALITY FOR SURVEILLANCE OF ACQUIRED IMMUNODEFICIENCY SYNDROME (AIDS) AND INFECTION WITH HUMAN IMMUNODEFICIENCY VIRUS (HIV) AND SURVEILLANCE-RELATED DATA (INCLUDING SURVEILLANCE INFORMATION, CASE INVESTIGATIONS AND SUPPLEMENTAL SURVEILLANCE PROJECTS, RESEARCH ACTIVITIES, AND EVALUATIONS)

The national surveillance program for HIV/AIDS is being coordinated by the Surveillance Branch of the Division of HIV/AIDS Prevention - Surveillance and Epidemiology (DHAP - SE), the National Center for HIV/STD/TB Prevention, a component of the Centers for Disease Control and Prevention (CDC), an agency of the United States Department of Health and Human Services. The surveillance information requested by CDC consists of reports of persons with suspected or confirmed AIDS or HIV infection, including children born to mothers infected with HIV, and reports of persons enrolled in studies designed to evaluate the surveillance program. The information collected by CDC is abstracted from laboratory, clinical, and other medical or public health records of suspected or confirmed HIV/AIDS cases; and from surveys that interview persons in recognized HIV risk groups or known to have a diagnosis of HIV/AIDS.

Surveillance data collection is conducted by State and Territorial health departments which forward information to CDC after deleting patient and physician names and other identifying or locating information. Records maintained by CDC are identified by computer-generated codes, patient date of birth, and a state/city assigned patient identification number. The data are used for statistical summaries and research by CDC scientists and cooperating state and local health officials to understand and control the spread of HIV/AIDS. In rare instances, expert CDC staff, at the invitation of state or local health departments, may participate in research or case investigations of unusual transmission circumstances or cases of potential threat to the public health. In these instances, CDC staff may collect and maintain information that could directly identify individuals.

Information collected by CDC under Section 306 of the Public Health Service Act (42 U.S.C. 242k) as part of the HIV/AIDS surveillance system that would permit direct or indirect identification of any individual or institution on whom a record is maintained, and any identifiable information collected during the course of an investigation on either persons supplying the information or persons described in it, is collected with a guarantee that it will be held in confidence, will be used only for the purposes stated in this

Assurance, and will not otherwise be disclosed or released without the consent of the individual or institution in accordance with Section 308 (d) of the Public Health Service Act (42 U.S.C. 242m(d)). This protection lasts forever, even after death.

Information that could be used to identify any individual or institution on whom a record is maintained by CDC will be kept confidential. Full names, addresses, social security numbers, and telephone numbers will not be reported to this national HIV/AIDS surveillance system. Medical, personal, and lifestyle information about the individual, and a computer-generated patient code will be collected.

Surveillance information reported to CDC will be used without identifiers primarily for statistical and analytic summaries and for evaluations of the surveillance program in which no individual or institution on whom a record is maintained can be identified, and secondarily, for special research investigations of the characteristics of populations suspected or confirmed to be at increased risk for infection with HIV and of the natural history and epidemiology of HIV/AIDS. When necessary for confirming surveillance information or in the interest of public health and disease prevention, CDC may confirm information contained in case reports or may notify other medical personnel or health officials of such information; in each instance, only the minimum information necessary will be disclosed.

No CDC HIV/AIDS surveillance or research information that could be used to identify any individual or institution on whom a record is maintained, either directly or indirectly, will be made available to anyone for non-public health purposes. In particular, such information will not be disclosed to the public; to family members; to parties involved in civil, criminal, or administrative litigation, or for commercial purposes; to agencies of the federal, state, or local government. Data will only be released to the public, to other components of CDC, or to agencies of the federal, state, or local government for public health purposes in accordance with the policies for data release established by the Council of State and Territorial Epidemiologists.

Information in this surveillance system will be kept confidential. Only authorized employees of DHAP - SE in the Surveillance Branch and Statistics and Data Management Branch, their contractors, guest researchers, fellows, visiting scientists, research interns and graduate students who participate in activities jointly approved by CDC and the sponsoring academic institution, and the like, will have access to the information. Authorized individuals are required to handle the information in accordance with procedures outlined in the Confidentiality Security Statement for Surveillance of Acquired Immunodeficiency Syndrome (AIDS) and Infection with Human Immunodeficiency Virus (HIV) and Surveillance-Related Data (Including Surveillance Information, Case Investigations and Supplemental Surveillance Projects, Research Activities, and Evaluations).

Appendix L

Guidelines for HIV/AIDS Surveillance

Note: This appendix is a copy of the *Technical Guidance for HIV/AIDS Surveillance Programs, Volume III: Security and Confidentiality Guidelines*. The guidelines were distributed in 2006 by the HIV Incidence and Case Surveillance Branch, Division of HIV/AIDS Prevention-Surveillance and Epidemiology, National Center for HIV, STD, and TB Prevention, Centers for Disease Control and Prevention.

The reference for this document is as follows:

Centers for Disease Control and Prevention and Council of State and Territorial Epidemiologists. *Technical Guidance for HIV/AIDS Surveillance Programs, Volume III: Security and Confidentiality Guidelines*. 2006.

Technical Guidance for HIV/AIDS Surveillance Programs

Volume III: Security and Confidentiality Guidelines



DEPARTMENT OF HEALTH AND HUMAN SERVICES
Centers for Disease Control and Prevention



All material contained in this document is in the public domain and may be used and reprinted without permission; citation of the source is, however, appreciated.

Suggested Citation

Centers for Disease Control and Prevention and Council of State and Territorial Epidemiologists. *Technical Guidance for HIV/AIDS Surveillance Programs, Volume III: Security and Confidentiality Guidelines*. Atlanta, Georgia: Centers for Disease Control and Prevention; 2006.

The document is available at <http://www.cdc.gov/hiv/surveillance.htm>.

Contents — Security and Confidentiality

Introduction	1-1
Existing Protections.....	1-1
Purpose of Guidelines.....	1-2
Policies.....	1-5
Scope.....	1-2
Requirements and Standards	1-3
Guiding Principles.....	1-4
Responsibilities	1-9
Training	1-11
Physical Security.....	1-11
Data Security.....	1-13
Data Movement	1-14
Sending Data to CDC	1-17
Transferring Data between Sites	1-18
Local Access.....	1-18
Central, Decentral, and Remote Access.....	1-22
Security Breaches	1-23
Laptops and Portable Devices	1-24
Removable and External Storage Devices.....	1-26
Attachment A.....	1-27
Attachment B.....	1-33
Attachment C	1-39
Attachment D	1-41
Attachment E.....	1-43
Attachment F	1-51
Attachment G	1-69
Attachment H	1-81

Contributors

This document, *Technical Guidance for HIV/AIDS Surveillance Programs*, was developed by the HIV Incidence and Case Surveillance Branch of the Division of HIV/AIDS Prevention, National Center for HIV, STD, and TB Prevention, Centers for Disease Control and Prevention in collaboration with the Council of State and Territorial Epidemiologists. The CDC/CSTE Advisory Committee provided oversight and leadership throughout the entire process. Workgroup contributors consisted of state and local health department representatives. Irene Hall, CDC, and Eve Mokotoff, CSTE, led the development.

Members of the CDC/CSTE Advisory Committee

CDC: Pamela Gruduah, Irene Hall, Martha Miller

CSTE: Gordon Bunch, California; Dena Ellison, Virginia; Jim Kent, Washington; Eve Mokotoff, Michigan; Stanley See, Texas

Chairs of Workgroups, CDC

Michael Campsmith, Data Analysis and Dissemination

Sam Costa, Security and Confidentiality

Irene Hall, Data Quality

Laurie Kamimoto, Electronic Reporting

Lata Kumar, Data Dictionary

Martha Miller, Overview

Kathleen McDavid, HIV Risk Factor Ascertainment

Ruby Phelps, Case Residency Assignment

Richard Selik, Death Ascertainment

Richard Selik, Record Linkage

Suzanne Whitmore, Perinatal and Pediatric Case Surveillance

CDC Contributors

Lori Armstrong, Mi Chen, Betsey Dunaway, John Gerstle, Kate Glynn, Irene Hall, Felicia Hardnett, David Hurst, Jennie Johnston, Danielle Kahn, Tebitha Kajese, Laurie Kamimoto, Kevin Lyday, Martha Miller, Andy Mitsch, Michelle Pan, Richard Selik, Amanda Smith, Damien Suggs, Patricia Sweeney, Kimberly Todd, Will Wheeler, Suzanne Whitmore, Irum Zaidi.

State and Local Health Department Contributors and Reviewers

Alabama: Anthony Merriweather, Danna Strickland; ***California-Los Angeles:*** Gordon Bunch, Mi Suk Harlan, Virginia Hu, Ann Nakamura; ***California-San Francisco:*** Ling Hsu, Maree Kay Parisi, Sandra Schwarcz; ***District of Columbia:*** Gail Hansen, Kompan Ngamsnga; ***Florida:*** Becky Grigg, Lorene Maddox; ***Illinois-Chicago:*** Margarita Reina; ***Indiana:*** Jerry Burkman; ***Iowa:*** Randy Mayer; ***Louisiana:*** Joseph Foxhood, Greg Gaines, William Robinson, Debbie Wendell, Amy Zapata; ***Massachusetts:*** Maria Regina Barros;

Michigan: Elizabeth Hamilton, Nilsa Mack, Eve Mokotoff, Yolande Moore;
Minnesota: Luisa Pessoa-Brandao, Tracy Sides; **New Hampshire:** Chris Adamski;
New Jersey: Wogayehu Afework, Linda Dimasi, Abdel Ibrahim, John Ryan; **New York City:** Melissa Pfeiffer, Judy Sackoff; **New York State:** Alexa Bontempo, Kathleen Brousseau, Donna Glebatis; **Ohio:** Sandhya Ramachandran; **Oklahoma:** Mark Turner;
Pennsylvania: Bonnie Krampe, Ming Wei; **South Carolina:** Dana Giurgiutiu; **Texas:** Thomas Barnabas, Dianna Highberg, Roy Reyna, Stanley See, Jan Veenstra; **Virginia:** Dena Ellison; **Washington:** Maria Courogen; **Washington-Seattle & King County:** Amy Bauer, Jim Kent; **Wisconsin:** Loujean Steenberg.

HIV/AIDS Surveillance Guidelines — Security and Confidentiality

Introduction

This document supersedes the October 1998 version of “Guidelines for HIV/AIDS Surveillance, Appendix C: Security and Confidentiality.” It reflects CDC's recommendation as best practices for protecting HIV/AIDS surveillance data and information. It details program requirements and security recommendations.

These requirements, recommendations, and practices are based on discussions with HIV/AIDS surveillance coordinators, CDC's Divisions of STD Prevention and TB Elimination, and security and computer staff in other Centers and Offices within CDC, and on reviews by state and local surveillance programs.

This document requires each cooperative agreement grantee to designate an Overall Responsible Party (ORP). The ORP will have the responsibility for the security of the surveillance system (including processes, data, information, software, and hardware) and may have liability for any breach of confidentiality. The ORP should be a high-ranking public health official. This official should have the authority to make decisions about surveillance operations that may affect programs outside of HIV/AIDS surveillance. The ORP is responsible for determining how surveillance information will be protected when it is collected, stored, analyzed, released, and dispositioned.

Although there are many sources of surveillance information (e.g., medical charts, insurance forms, behavioral surveys, and service organizations), the authority of this document is limited to data collected for HIV/AIDS surveillance. Data in the HIV/AIDS surveillance system are to be held under the highest scrutiny and require the most stringent protections, regardless of the level of security of the source data or of non-HIV surveillance data. A breach of confidentiality anywhere in this system could affect surveillance operations nationwide. All references in these guidelines to surveillance information and data should be understood to refer only to HIV/AIDS-related surveillance. These security guidelines may serve as a model for other programs to emulate when reviewing or upgrading security protocols that are specific to their overall procedures and mission. For programs that integrate HIV and other disease surveillance, all data should be protected equally in compliance with these guidelines.

This document is intended to assist programs in providing aggregate data for maximum public health utility with minimum risk of disclosure of individual-level data. Given the advances in information technology, as well as changes in surveillance practices since the previous update in 1998, the guidelines are being updated to provide project areas with guidance reflecting those changes. CDC will continue to assist states as they adapt their policies and procedures to comply with evolving requirements and standards.

Existing Protections

HIV/AIDS surveillance is the joint responsibility of many participants in the health care system. Among the participants are state and local health department surveillance programs; public and private institutions providing clinical, counseling, and laboratory services; individual health care providers; persons at risk for HIV infection; and persons

with HIV or AIDS. The ability of state and local surveillance programs to collect, store, use, and transmit sensitive HIV/AIDS case information in a secure and confidential manner is central to the program's acceptability and success. The importance of data security has been a long-established component of these guidelines. Various federal and state statutes, regulations, and case law provide legal protection of HIV/AIDS surveillance information. Among these safeguards are a right to informational privacy under the Fifth and Fourteenth Amendments to the Constitution, and federal assurance of confidentiality (under § 308(d) of the Public Health Service Act and various state and local protections).

The dynamic nature of information technology is a critical consideration in developing security policies and procedures that will be used to meet the requirements and standards described in these guidelines. The HIV/AIDS surveillance system was created before the development of technologies such as laptops, portable external storage devices, and the Internet, all of which can be potential sources for security breaches. Now, all state and local health departments should routinely assess the changing world of computer technology and adjust security policies and procedures to protect against potential new risks. CDC is available to provide technical consultation on technology and security issues.

Purpose of Guidelines

Scope

The security standards presented here are intended to apply to local, state, and territorial staff and contractors funded through CDC to perform HIV/AIDS surveillance activities and at all sites where an HIV/AIDS reporting system is maintained.

Although designed for HIV/AIDS surveillance activities, these security standards may serve as a model for other programs to use in reviewing or upgrading security protocols that are appropriate for their overall procedures and mission. Although health care providers who are the source of surveillance information are not under an obligation to follow these security standards, local and state surveillance staff may nevertheless suggest portions of these standards to providers to foster a shared stewardship of sensitive information by promoting security and confidentiality protections in provider settings.

Providers concerned with the Health Insurance Portability and Accountability Act (HIPAA) may use these guidelines as a foundation for their HIPAA compliance policies; however, these guidelines are not a guarantee of HIPAA compliance within a provider setting. Providers need to use their own resources to evaluate their everyday compliance. HIV/AIDS surveillance programs should remind providers that HIPAA permits public health reporting requirements and that providers are still subject to relevant laws, regulations, and public health practices, as described in the MMWR available from <http://www.cdc.gov/mmwr/PDF/wk/mm52SU01.pdf>. Surveillance staff can also find answers to many frequently asked questions regarding HIPAA and public health at the Office of Civil Rights Web site at <http://www.hhs.gov/ocr/hipaa>.

The HIV/AIDS surveillance system was not designed for case management purposes, and CDC does not provide surveillance funds to states to support case management or referral services. However, some states and territories have chosen to use information from

individual case reports to offer voluntary referrals to prevention and care services, including partner notification assistance. The confidentiality and security issues associated with the provision of those services are outside the scope of this document. When considering such releases of individual-level data from the HIV/AIDS reporting system to other HIV prevention and care programs, state and local health officials should have mechanisms in place to inform and receive input from community members, such as prevention planning groups. Officials must require that recipients of surveillance information have well-defined public health objectives and that they have compared the effectiveness of using confidential surveillance data in meeting those objectives with other strategies. Furthermore, recipients of surveillance information must be subject to the same training and penalties for unauthorized disclosure as surveillance staff.

Data collected by sites through surveillance activities and reported to CDC originate in health care provider, institutional, and laboratory settings. From these sources, confidential information on persons with HIV/AIDS may be obtained in accordance with state law, regulation, or rule. The convenience of having HIV/AIDS surveillance data should not be considered a justification for using it for nonpublic health purposes in preference to more appropriate sources of individual-level data. State and local HIV/AIDS surveillance programs must develop data release policies that include restrictions on the use of surveillance data for nonpublic health purposes. Refer to the [Policies](#) section of this document for policy requirements.

A separate set of protections covers HIV/AIDS surveillance information and data maintained at CDC. To protect the confidentiality of persons reported with HIV/AIDS, local and state surveillance program staff do not send names and other specific identifying information to CDC. Additional protections are provided by exemptions to the Freedom of Information Act of 1966 (specifically U.S.C. 552(b)[6]) and by the Privacy Act of 1974. Most importantly, the Assurance of Confidentiality authorized by 308(d) of the Public Health Service Act enables CDC to withhold disclosure of any HIV/AIDS surveillance-related information. A copy of the Assurance of Confidentiality statement can be found in [Attachment D](#). Any HIV/AIDS-related human subject research (as distinguished from routine HIV/AIDS surveillance) conducted or supported by CDC must be approved by an Institutional Review Board (IRB). A key condition of IRB approval is that provisions must be in place to protect the privacy of subjects and to maintain the confidentiality of data.

Requirements and Standards

The requirements and standards in this document are designed for state and local HIV/AIDS surveillance agencies to use as both a guide to the surveillance staff and a basis for corrective action when conduct falls below the required minimum standards as stated in the various requirements. These guidelines also define the standard of conduct that the public should expect of HIV/AIDS surveillance staff in protecting private and sensitive information. Attending to the details of good public health practice creates a professional environment for surveillance staff. Good public health practice dictates that HIV/AIDS surveillance data are used only for the purposes for which they were collected.

This document is divided into security-related topics. Each topic contains both program requirements and discussions that serve to either explain the requirement or offer security considerations that will help comply with the requirement.

Program requirements are mandatory, and the ORP will certify them annually. See [Requirement 10](#). Each requirement states the minimum standard that surveillance staff must achieve. Falling below this standard could result in corrective action. These standards do not prescribe the penalty that should result from a violation of a program requirement. The ORP, considering the nature of the offense, the surrounding circumstances, local policy, and state law, should determine those decisions. Discipline may range from an employee reprimand to criminal charges.

Additional security considerations, unlike the program requirements, are aspirational and represent the objectives that each member of the surveillance staff should strive to achieve. They comprise a body of principles that surveillance staff can rely upon for guidance in many specific situations. For a list of additional security considerations, refer to [Attachment A: Additional Laptop Security Considerations](#) and [Attachment B: Additional Security and Policy Considerations](#).

Guiding Principles

The five guiding principles listed next are the backbone upon which all program requirements and security considerations are derived. The applicable guiding principle is referenced at the end of each program requirement (e.g., GP-1), so a reader can determine the principle that is being addressed by the requirement.

Guiding Principle 1

HIV/AIDS surveillance information and data will be maintained in a physically secure environment. Refer to sections [Physical Security](#) and [Removable and External Storage Devices](#).

Guiding Principle 2

Electronic HIV/AIDS surveillance data will be held in a technically secure environment, with the number of data repositories and individuals permitted access kept to a minimum. Operational security procedures will be implemented and documented to minimize the number of staff that have access to personal identifiers and to minimize the number of locations where personal identifiers are stored. Refer to sections [Policies](#), [Training](#), [Data Security](#), [Access Control](#), [Laptops and Portable Devices](#), and [Removable and External Storage Devices](#).

Guiding Principle 3

Individual surveillance staff members and persons authorized to access case-specific information will be responsible for protecting confidential HIV/AIDS surveillance information and data. Refer to sections [Responsibilities](#), [Training](#), and [Removable and External Storage Devices](#).

Guiding Principle 4

Security breaches of HIV/AIDS surveillance information or data will be investigated thoroughly, and sanctions imposed as appropriate. Refer to section [Security Breaches](#).

Guiding Principle 5

Security practices and written policies will be continuously reviewed, assessed, and as necessary, changed to improve the protection of confidential HIV/AIDS surveillance information and data. Refer to sections [Policies](#) and [Security and Confidentiality Program Requirement Checklist](#).

Also included in the document are a series of attachments that provide specific information on various topics that would be either too detailed or inappropriate in the body of this document. The following eight documents are attached:

[Attachment A: Additional Laptop Security Considerations](#)

[Attachment B: Additional Security and Policy Considerations](#)

[Attachment C: Federal Encryption Standards](#)

[Attachment D: CDC Assurance of Confidentiality](#)

[Attachment E: Sample Employee Oath - Texas](#)

[Sample Employee Oath - Seattle/King County](#)

[Sample Employee Oath - Louisiana](#)

[Attachment F: Glossary of Surveillance and Technical Terms](#)

[Attachment G: Using HIV Surveillance Data to Document Need and Initiate Referrals](#)

[Attachment H: Security and Confidentiality Program Requirement Checklist](#)

Policies

Requirement 1 Policies must be in writing. (GP-2)

Requirement 2 A policy must name the individual who is the Overall Responsible Party (ORP) for the security system. (GP-2)

The name of the individual who is designated as the ORP, rather than an organizational position, must be provided to CDC annually. The rationale is to increase accountability and help ensure that the individual knows his/her responsibilities as ORP.

Requirement 3 A policy must describe methods for the review of security practices for HIV/AIDS surveillance data. Included in the policy should be a requirement for an ongoing review of evolving technology to ensure that data remain secure. (GP-5)

As part of a review and quality improvement procedure, sites may consider a self-administered procedure by using the *Security and Confidentiality Program Requirement Checklist* shown in [Attachment H](#) (or a similar form tailored for local use) and refer to the log of breaches.

Requirement 4 Access to and uses of surveillance information or data must be defined in a data release policy. (GP-2)

Requirement 5 A policy must incorporate provisions to protect against public access to raw data or data tables that include small denominator populations that could be indirectly identifying. (GP-2)

Data release policies outline the types of data that can be released and who is authorized to receive the data. For example, with regard to matching HIV/AIDS cases to cases in other data stores (e.g., TB, STD, or vital statistics), the policy should specify what the purpose is, how this is done, who performs the matching, what results are released, how the results should be stored, and who receives the results.

This policy establishes the rules to be implemented to ensure that information is allowed to flow within the information system and across system boundaries only as authorized. Data release, by definition, suggests that information about an HIV-infected individual is available for distribution. A data release policy has to balance the inherent purpose of HIV/AIDS surveillance data with the confidentiality of any HIV-infected individual reported for surveillance purposes. Therefore, any HIV/AIDS surveillance data release policy must be written with two questions in mind. First, which data elements can be released about any case patient that would not identify the individual if pieced together? Second, what purposes are consistent with the reasons for which the data were originally collected?

With regard to the first question, certain information containing patient identifying data elements (including elements such as patient's name, address, and social security number) may never be released for public distribution. Care must also be taken to ensure that information released cannot be linked with other databases containing additional information that can be used to identify someone. However, in developing a data release policy, state and local HIV/AIDS surveillance programs should be aware that several data elements that are not inherently identifying could be linked together to identify an individual. For example, when releasing data on a community with relatively few members of a racial/ethnic group (e.g., Asian/Pacific Islanders or American Indians/Alaska Natives), a risk factor group (e.g., persons with hemophilia), or an age group (e.g., >50 years old or specifying the date of birth or death), surveillance staff should be careful that release of aggregate data on the distribution of HIV-infected individuals by these categories could not suggest the identity of an individual. Time periods also need to be considered when developing a data release policy. Output from cases reported cumulatively (since 1981) better hides any individual's identity than output from cases reported within the past 12 months. Therefore, care should be taken in deciding how both the numerator and the denominator are defined when developing a data release policy.

Traditionally, surveillance data are released as aggregated data. As a rule, CDC will not release national aggregated data in tables when the number of records reflected in a cell falls below a minimum size, depending on sensitivity of the data. Some states have similar cell size restrictions. Most states consider the denominator size of the population under analysis and may release small cells under certain circumstances. However, as described previously, even cell size limitations could allow for inferential identification of an individual. Care should also be taken in graphic presentation of data. For example, geographic information systems (GIS) allow for relatively accurate dot mapping of observations. Care must be taken that graphic (like numeric) presentation of data cannot permit the identification of any individual by noting pinpoint observations of HIV cases at, for example, the county, ZIP code, or census tract level. Other considerations in developing data release policies include the need for state surveillance programs to assure that their data release policies are consistent with state confidentiality laws, and to include clear definitions of terms used in the data release policy (e.g., personal identifier, population size, and time period). For a complete discussion covering this issue, refer to the chapter on *<Data Analysis and Dissemination>*.

The second issue that should guide the development of a data release policy is to consider the purpose for which the data were originally collected. To be consistent with the federal Assurance of Confidentiality under which CDC collects HIV data and the purpose for which CDC provides support to states to conduct surveillance, no HIV surveillance information that could be used to identify an individual should be available to anyone for nonpublic health purposes. Examples include the release of individual-level data to the public; to parties involved in civil, criminal, or administrative litigation; for commercial purposes; or to nonpublic health agencies of the federal, state, or local government. Surveillance data are collected to monitor trends in the epidemic on a population-based level. However, some state and local surveillance programs have chosen to share individual case reports with prevention and care programs to initiate referrals to services. Additionally, some surveillance programs use surveillance data to initiate follow-up for supplemental public health research. Programs that choose to establish these linkages should do so without compromising the quality or security of the surveillance system and should establish principles and procedures for such practices in collaboration with providers and community partners. Programs that receive surveillance information should be subject to the same penalties for unauthorized disclosure and must maintain the data in a secure and confidential manner consistent with CDC surveillance guidelines. Additionally, activities deemed to be research should get appropriate human subjects approvals consistent with state and local health department procedures. A discussion on using HIV surveillance data to initiate referrals to prevention or treatment services is available in the document *Integrating HIV and AIDS Surveillance: A Resource Manual for Surveillance Coordinators - Toolkit 5, Using HIV Surveillance Data to Document Need and Initiate Referrals*, found in [Attachment G](#). Several other CDC resources and guidance documents are available online to inform local discussions, including *HIV Partner Counseling and Referral Services: Guidance*, *HIV Prevention Case Management: Guidance*, resources on evaluation of HIV prevention programs, and more at <http://www.cdc.gov/hiv/pubs/guidelines.htm>. The HIV Incidence and

Case Surveillance Branch is currently working on ethical guidelines for the use of public health data for HIV/AIDS. Please contact your HIV surveillance program consultant for additional information on these guidelines.

Requirement 6 Policies must be readily accessible by any staff having access to confidential surveillance information or data at the central level and, if applicable, at noncentral sites. (GP-2)

As security questions arise in the course of surveillance activities, staff must have ready access to the written policies. In most circumstances, having a copy of the written policies located within the surveillance unit would satisfy this requirement. Computer access to an electronic version of the policies also may be acceptable. The key is for staff to have quick access to policies as security and confidentiality questions arise.

Requirement 7 A policy must define the roles for all persons who are authorized to access what specific information and, for those staff outside the surveillance unit, what standard procedures or methods will be used when access is determined to be necessary. (GP-2)

Requirement 8 All authorized staff must annually sign a confidentiality statement. Newly hired staff must sign a confidentiality statement before access to surveillance data is authorized. The new employee or newly authorized staff must show the signed confidentiality statement to the grantor of passwords and keys before passwords and keys are assigned. This statement must indicate that the employee understands and agrees that surveillance information or data will not be released to any individual not granted access by the ORP. The original statement must be held in the employee's personnel file and a copy given to the employee. (GP-2)

The policy should establish rules to ensure that only designated individuals, under specified conditions, can

- Access the information system (network logon, establish connection),
- Activate specific system commands (execute specific programs and procedures; create, view, or modify specific objects, programs, information system parameters). The policy should include provisions for periodic review of access authorizations. Note that CDC's HIV/AIDS Reporting System does not have the ability within the application to establish access times.

The policy could limit access to sensitive data to specified hours and days of the week. It should also state types of access needed, which could be linked to roles defined for those with access. For example, epidemiologists may have access to data across programs that do not include identifiers.

Additionally, the policy should cover restrictions on access to the public Internet or e-mail applications while accessing surveillance information. Accidental transmission of data through either of these systems can be avoided if they are never accessed simultaneously. Similarly, intruders can be stymied in attempts to access information if it is not available while that connection is open.

The policy should establish rules that ensure that group authenticators (administrators, super users, etc.) are used for information system access only when explicitly authorized and in conjunction with other authenticators as appropriate. The policy should express similar rules for individual users to ensure that access to identifiable data is allowed only when explicitly authorized and in conjunction with other authenticators as appropriate. The policy should document the process for assigning authorization and identify those with approval authority. Information technology (IT) authorities granting access must obtain approval from the ORP or designee before adding users, and they should maintain logs documenting authorized users. The ORP or a designee should periodically review user logs.

Requirement 9 A policy must outline procedures for handling incoming mail to and outgoing mail from the surveillance unit. The amount and sensitivity of information contained in any one piece of mail must be kept to a minimum. (GP-2)

The U.S. Mail and other carrier services are commonly used for the movement of paper copies of information. There are many ways that project areas can protect the confidentiality of an HIV-infected individual when using the mail. For example, when surveillance staff and providers are mailing information (e.g., case report forms) to the central office, the policy could require that names and corresponding patient numbers be sent in one envelope, while the remaining information referenced by the corresponding patient number is sent in another envelope. In addition, the terms 'HIV' or 'AIDS' should not necessarily be included in either the mailing address or the return address. Mailing labels or pre-addressed, stamped envelopes may be supplied to field staff and providers to encourage this practice and to ensure the use of the correct mailing address. Whenever confidential information is mailed, double envelopes should be used, with the inside envelope clearly marked as confidential.

Because of the potential number of entries on a given paper copy line list, programs must exercise extreme caution if they find it necessary to mail a paper list. Procedures for mailing lists, including the amount and type of information permitted in any one mailing, must be clearly outlined in the local policy. Two methods that surveillance programs currently employ to minimize risk when using the mail are (1) to generate lists containing names without references to HIV or AIDS or (2) to remove the names from the list and mail them separately from the other sensitive information.

Responsibilities

Requirement 10 In compliance with CDC's cooperative agreement requirement, the ORP must certify annually that all program requirements are met. (GP-2)

Requirement 11 Each member of the surveillance staff and all persons described in this document who are authorized to access case-specific information must be knowledgeable about the organization's information security policies and procedures. (GP-3)

Requirement 12 All staff who are authorized to access surveillance data must be responsible for challenging those who are not authorized to access surveillance data. (GP-3)

Many programs consider the area of personal responsibility as a potential area of concern because the actions of individuals within a surveillance system are much more difficult to proscribe than operational practices. This area represents one of the most important aspects of holding data in a secure and confidential fashion, but the development of objective criteria for assessing the degree of personal responsibility in individual staff members may be difficult.

The program requirements in this area may be evaluated objectively by using a series of questions supervisors pose during the annual review of security measures with staff. Input from staff can be obtained through such questions as these:

- How often do you find the need to reference local or CDC security policies or standards?
- Do you know who (by job position or name) should have access to the secure surveillance area? How would you approach someone who was entering the secured room whom you believe was not authorized access? Have you had any occasion to challenge such a person?
- To whom should security irregularities be reported? What are some examples of what would constitute an irregularity? What irregularities would not need to be reported, if any?
- Who else needs access to your computer for any reason? For example, do family members or other staff members ever need to use your workstation? Do you ever need to lend your key to a secured area to another member of the health department staff for after-hours access to the building? Who else knows your computer passwords?

Requirement 13 All staff who are authorized to access surveillance data must be individually responsible for protecting their own workstation, laptop, or other devices associated with confidential surveillance information or data. This responsibility includes protecting keys, passwords, and codes that would allow access to confidential information or data. Staff must take care not to infect surveillance software with computer viruses and not to damage hardware through exposure to extreme heat or cold. (GP-3)

Surveillance staff should avoid situations that might allow unauthorized persons to overhear or see confidential surveillance information. For example, staff should never discuss confidential surveillance information in the presence of persons who are not authorized to access the data. Staff working with personal identifiers should have a

workspace that does not allow phone conversations to be overheard or paperwork and computer monitors to be observed by unauthorized personnel. Ideally, only staff with similar roles and authorizations would be permitted in a secure, restricted area.

Training

Requirement 14 Every individual with access to surveillance data must attend security training annually. The date of training must be documented in the employee's personnel file. IT staff and contractors who require access to data must undergo the same training as surveillance staff and sign the same agreements. This requirement applies to any staff with access to servers, workstations, backup devices, etc. (GP-3)

Security training is required for all new staff and must be repeated annually thereafter, but the nature of this training may vary based on local circumstances. For example, in areas of low HIV prevalence where one surveillance person is on staff, if that person leaves before training a replacement, the policy should indicate that training for data security and confidentiality may be obtained in a neighboring state. In other areas, new staff may be trained by the surveillance coordinator one-on-one. In this instance, the policy should document what types of information must be covered in such a session, and provisions should be made to document that training was completed. In areas of high HIV prevalence with larger numbers of staff, periodic group training sessions may be more appropriate.

Physical Security

Requirement 15 All physical locations containing electronic or paper copies of surveillance data must be enclosed inside a locked, secured area with limited access. Workspace for individuals with access to surveillance information must also be within a secure locked area. (GP-1)

Requirement 16 Paper copies of surveillance information containing identifying information must be housed inside locked filed cabinets that are inside a locked room. (GP-1)

Requirement 17 Each member of the surveillance staff must shred documents containing confidential information before disposing of them. Shredders should be of commercial quality with a crosscutting feature. (GP-3)

Maximum security practice dictates that HIV/AIDS surveillance data be maintained on a dedicated file server at only one site in each project area where layers of security protections can be provided in a cost-effective manner. This would obviate the need to duplicate expensive security measures at multiple locations throughout the state.

Remote sites that need access to the central surveillance server for surveillance activities could access the server through a secured method (e.g., virtual private network [VPN], or authentication server) set up for authorized users. Analysis databases available to all intrastate jurisdictions would allow the data to be used for analysis and program planning at the local level. As resources permit, CDC technical

and financial assistance may be available to assist states in moving to a more centralized surveillance operation. See section [Central, Decentral, and Remote Access](#) for details.

CDC recognizes that, for some surveillance programs, it may not be possible at this time to limit the entry of HIV/AIDS data into a reporting system located at a single site. Based on local health department policies and organization, some states have decided to maintain the reporting system in more than one site. If this is the case, every additional reporting system site in the state must meet the same minimum security measures outlined in all of the program requirements.

Because the surveillance system can potentially identify any number of persons with HIV/AIDS within a state (or local jurisdiction if surveillance is decentralized), particular attention to the security of surveillance information is critical. CDC's requirement to house the surveillance information in a locked room is long standing and has been part of the surveillance guidance for many years. Jurisdictions use various security methods to hold HIV/AIDS case data stores, but the minimum security standard is to enclose the surveillance information inside a locked room regardless of the method used. Whether the reporting system resides on a server or workstation, the computer containing the electronic surveillance data must be enclosed inside a locked room. Only authorized surveillance personnel should have access to the locked room. However, depending on the numbers of HIV/AIDS cases reported, the size and role of the surveillance staff, community interest, and health department resources, the ORP may decide that other authorized health department staff may need to work inside the surveillance room.

If the surveillance data reside on a server inside a locked room and not on the hard drive of any individual workstation within the department, the individual workstation (when logged off the network) does not pose a great security risk and would not necessarily have to be located behind a locked door to meet the minimum standard. However, most health departments using Local Area Network (LAN) systems to maintain surveillance data require both the workstation and the server to be located in rooms with doors that lock. LAN accounts with access to identifying information in the reporting system should be limited only to the workstations of those authorized. LAN accounts also should be limited by time of day. See [Requirement 7](#).

The use of cubicles in many office buildings can also present a challenge to creation of a secure area. Cubicles with low walls make it difficult, even within a secure area, to have a telephone conversation without others hearing parts of the conversation. Where necessary, higher cubicle walls with additional soundproofing can be used. When cubicles are part of the office structure, cubicles where sensitive information is viewed, discussed, or is otherwise present should be separated from cubicles where staff without access to this information are located.

When electronic surveillance data with personal identifiers are stored outside of a physically secure area (i.e., a locked room with limited access), or if limited local resources require that surveillance data with personal identifiers stored on a LAN be accessible to nonsurveillance staff, real-time encryption software must be employed. The additional encryption software is designed to keep identifying information

encrypted. Should an unauthorized individual gain access to the surveillance database, unencrypted identifying information cannot be viewed. Encryption software that meets federal standards must be used before data are transmitted to CDC. See [Attachment C: Federal Encryption Standards](#) and section [Sending Data to CDC](#) for details. Encryption requirements would also apply to backup storage media, which are frequently located off-site and could be managed by an outside vendor.

Paper copy data stores must be maintained in a locked cabinet and inside a locked room. If an area chooses to no longer maintain paper copies in locked file cabinets inside a locked room (e.g., because of age or volume), the program should destroy the completed forms after ensuring the data are entered into the reporting system and after they are no longer needed for follow-up. Before destroying the forms, a site may opt to digitally scan forms for future reference. Digitized forms should be secured the same as any other surveillance data. [Requirement 15](#) does not apply to subsets of case report forms, such as those that a surveillance staff member may hold in the course of an investigation, but does apply to paper copy line lists or logbooks that list a large number of reported cases by name in any one jurisdiction. Even if appropriate space is available to properly store all surveillance forms, program staff should consider developing a records retention policy that would describe the record retention and the scheduling of records for destruction after a designated period. Older records offer only limited value, but continue to pose a security risk. Sites should carefully weigh the benefits and risks of retaining any paper copies of case report forms. Such a decision should be predicated on adherence to these security standards, state regulations, and local practice. Once a decision has been made to destroy a case report form, line list, notes, or any other related paper surveillance document, the document must be destroyed in accordance with [Requirement 17](#).

Requirement 18 Rooms containing surveillance data must not be easily accessible by window. (GP-1)

Window access, for the purposes of this document, is defined as having a window that could allow easy entry into a room containing surveillance data. This does not mean that the room cannot have windows; rather, windows need to be secure. If windows cannot be made secure, surveillance data must be moved to a secure location to meet this requirement.

A window with access, for example, may be one that opens and is on the first floor. To secure such a window, a permanent seal or a security alarm may be installed on the window itself. Even if the window does not open, program managers may decide to include extra precautions if, for example, the building does not have security patrols or if the building or neighboring buildings have had breaches. If a project area has a concern about a current or planned physical location, staff can request advice from CDC.

Data Security

For the purposes of this document, a remote site is defined as a site that remotely connects to and accesses a centralized electronic database to enter and store surveillance data even though paper forms may be stored locally. The central database is located in a different

physical location than the remote site and usually in a different city. A satellite location is defined as a site that collects and electronically enters surveillance data in a local database and then sends the electronic data file to a central location. If remote and satellite sites maintain case report forms or other surveillance information with personal identifiers, the central location should not be maintaining duplicate copies of the case report forms. Surveillance staff should discourage providers from maintaining duplicate copies of HIV/AIDS case reports after they have been reported to the health department.

The statewide HIV/AIDS case database should be housed in only one location (excluding electronic backups and replication for disaster recovery); however, as states with multiple database locations move to more centralized operations, the number of satellite locations within a state should be kept to a minimum, thereby keeping the data collection and storage as centralized as possible. If the system is decentralized, each remote and satellite site should maintain only cases within that site's jurisdiction, and must meet the same physical security requirements discussed in section [Physical Security](#).

If, after discussing a records retention schedule, program staff decide to retain the hard copy case report form even after the record is entered into the reporting system, they should consider removing or striking out the name on the report before storage. The state patient number would still provide linkage, when necessary, to the name in the reporting system while improving record security. This practice would decrease (1) the number of places where names are stored, (2) the amount of time they are held, and (3) the number of persons who may have access to them in the future.

Security software that controls the storage, removal, and use of data maintained in the reporting system should be in place at all locations where the electronic surveillance data are maintained. Security software may include such protections as user identifications, passwords, boot protection, encryption algorithms, and digital signatures. Additionally, an area may maintain names outside of the reporting system and use a state ID number to link name and surveillance information when needed.

Data Movement

Requirement 19 Surveillance information must have personal identifiers removed (an analysis dataset) if taken out of the secured area or accessed from an unsecured area. (GP-1)

Requirement 20 An analysis dataset must be held securely by using protective software (i.e., software that controls the storage, removal, and use of the data). (GP-1)

Requirement 21 Data transfers and methods for data collection must be approved by the ORP and incorporate the use of access controls. Confidential surveillance data or information must be encrypted before electronic transfer. Ancillary databases or other electronic files used by surveillance also need to be encrypted when not in use. (GP-1)

Electronic files stored for use by authorized surveillance staff should be encrypted until they are actually needed. If these files are needed outside of the secure area, real-time encryption or an equivalent method of protection is required.

This requirement also applies in those situations where surveillance data are obtained electronically from external sources (clinical data management systems and laboratories) or as part of a separate health department data collection system (Careware for example). Extracts from those systems need to be protected as if they were extracts from the surveillance data system. Additionally, those systems within the health department need to be held to the same standards as the HIV/AIDS surveillance systems. External agencies are to be encouraged to review their procedures, and approved data transfer methods need to be used.

Requirement 22 When case-specific information is electronically transmitted, any transmission that does not incorporate the use of an encryption package meeting the Advanced Encryption Standard (AES) encryption standards and approved by the ORP must not contain identifying information or use terms easily associated with HIV/AIDS. The terms HIV or AIDS, or specific behavioral information must not appear anywhere in the context of the communication, including the sender and/or recipient address and label. (GP-2)

The intent of this requirement is to eliminate the possibility that a third party may identify a person as being a member of an HIV risk factor group or HIV infected. For example, when trying to locate an HIV-infected person during an NIR (No Identified Risk) investigation or interview, do not send letters or leave business cards or voice messages at the person's residence that include any terminology that could be associated with HIV, AIDS, or the health department. These precautions need to be taken in case a family member or friend discovers the letter or card or hears the voice message. Similarly, if a third party calls the telephone number listed on a card or letter, that party should not be able to determine by a phone greeting that it is an HIV/AIDS surveillance unit (or the health department); nor should a third party be able to obtain that information by pretending to be the case patient. This may require the use of some confirmation mechanism to assure that the person calling really is the case patient and not someone pretending to be that person to discover confidential information. For additional information on confidential interview techniques, you may request CDC interview guidelines by contacting your CDC program consultant.

If secure fax or encrypted e-mail transmissions are used at all (although CDC strongly discourages their use), care must be taken to avoid linking HIV or risk factor status with identifiable information about a person. This may include ensuring that the terms HIV or AIDS do not appear in the fine print at the very top of a fax indicating who sent it and that these terms do not appear in more obvious locations in the letterhead and body of the fax. Other important steps include thinking about who else besides the intended recipient may have access to faxes on the receiving end and the possibility of misdialing the fax number or using the incorrect e-mail address.

Requirement 23 When identifying information is taken from secured areas and included on line lists or supporting notes, in either electronic or hard copy format, these documents must contain only the minimum amount of information necessary for completing a given task and, where possible, must be coded to disguise any information that could easily be associated with HIV or AIDS. (GP-1)

One purpose of this requirement is to make it difficult to link an individual's name on a line list with HIV/AIDS should that line list fall into the hands of an unauthorized person. Terms that could be associated with HIV/AIDS include CD4 count or opportunistic infection (OI). Programs should consider using less recognizable terms, codes, or abbreviations such as T-lymphocyte count or OI. In some circumstances, just the word "count" may suffice. While risk factor information (e.g., injection drug use or sexual orientation) may not necessarily be associated with HIV/AIDS, it nevertheless is highly sensitive. Wherever possible, risk factor categories must be coded to help minimize the possibility of a breach. A coding scheme for transmission category is already built into the reporting system and should be used when there is a need to generate line lists with risk factor categories. When surveillance staff write notes, they should make it a habit to use these risk factor codes. For example, instead of using the phrase injection drug user or the readily decipherable abbreviation IDU, a code could be substituted.

This requirement applies to information or data taken from secure areas. It does not refer to data collected from the field and taken to secure areas. While coding of terms associated with HIV/AIDS in the field is encouraged, there may be occasions when it cannot be done, for example, when uncoded terminology must be abstracted from a medical chart on a No Identified Risk case during the course of an investigation.

Requirement 24 Surveillance information with personal identifiers must not be taken to private residences unless specific documented permission is received from the surveillance coordinator. (GP-1)

Under exceptional circumstances, HIV/AIDS surveillance information with personal identifiers may be taken to private residences without approval if an unforeseen situation arises that would make returning to the surveillance office impossible or unsafe. For example, if a worker carrying sensitive information were caught in a sudden heavy snowstorm, driving home instead of returning to the office would be permissible provided the worker's supervisor is notified (or an attempt was made to notify the supervisor) of the need to return home with the sensitive information. Precautions should be taken at the worker's home to protect the information under such circumstances. All completed, or partially completed, paper case report forms should be transported in a locked satchel or briefcase.

Managing field time effectively can be accomplished by using a variety of creative tactics. Field visits should be scheduled in the most efficient way possible. One option is to assign provider sites to workers by geographic area. For example, all providers in the east sector could be covered by the same worker to minimize travel time between sites. Another option might be to schedule visits so that sites located far from the

office receive visits early in the day with staff working their way back to the office by the end of the day. A flextime schedule is another option that a site may wish to consider.

If returning to the secured area creates significant inefficiencies in case surveillance investigations, alternative methods of securing sensitive surveillance information could be considered when developing the policy that satisfies this requirement. Investigators could incorporate the use of pre-addressed, stamped envelopes and drop completed case report forms in the mail before returning home for the day. Tampering with the mail is a felony, and case reports are considered better protected in the mail than at a private residence. This possibility should be accounted for when developing the mail policy discussed in [Requirement 9](#).

Some areas do not complete case report forms on-site, but take notes using shorthand that is not easily translated and does not contain HIV-related terms. Notes such as these could be stored in less secure areas because someone seeing the notes would not understand their meaning. When this method is used, blank case report forms or other HIV-related materials should not be stored at the same location as the notes. Staff using this technique may carry the notes around discreetly (e.g., in a purse or notebook) and then complete official forms when they return to the surveillance office. Other methods to disguise the data, de-identify it, or separate sensitive variables from it could be used to eliminate the need to return to the office at the close of business (i.e., if personal identifiers are removed using approved methods, the information is less sensitive and may be secured off-site). Whatever methods are used, the approved method must be described in the local security policy.

Requirement 25 Prior approval must be obtained from the surveillance coordinator when planned business travel precludes the return of surveillance information with personal identifiers to the secured area by the close of business on the same day. (GP-1)

Policies and procedures for gaining prior approval for not returning surveillance information with personal identifiers to the secured area at the close of each business should be implemented. Refer to the discussion following [Requirement 24](#) for additional considerations.

Sending Data to CDC

CDC's policy requires encryption when any moderately or highly sensitive files, any moderately or highly critical information, or any limited access/proprietary information is to be transmitted to or from CDC either electronically or physically. All data that meet these criteria must be encrypted using the Advanced Encryption Standard (AES). See [Attachment C](#) for details describing federal encryption standards. Currently, CDC requires that this category of electronic data be sent via its Secure Data Network (SDN). Future considerations may include sending data using the Public Health Information Network Messaging System (PHIN MS). The SDN uses digital certificate technology to create a Secure Sockets Layer (SSL) or encrypted tunnel through which data are transmitted. The SSL is broken once the client browser loses connectivity with the CDC Web server, which is located outside of its firewall.

To protect sensitive data once the SSL is broken and as they move between various CDC servers, CDC requires that sensitive data be encrypted with a product that meets federal standards. To support that requirement, CDC can provide users with a free CDC-produced, Java-based software called SEAL. Some CDC programs will also accept files encrypted with commercially available products. A site must coordinate efforts with CDC if the site wishes to use a commercially available encryption product. Any commercially available product selected must meet federal AES standards.

Note: The HIV/AIDS Reporting System (HARS) transfer files are output with a 40-bit encryption algorithm that does not meet the standards. Therefore, HARS files must be encrypted before being sent to CDC via the SDN. The e-HARS transfer files are output with a 1024-bit SEAL encrypted algorithm that does meet the standards, and, therefore, no additional encryption will be necessary before sending to CDC.

Transferring Data between Sites

Many sites have a need to move data within a state or between states. If these data meet the criteria described in the previous topic, [Sending Data to CDC](#), CDC strongly recommends that these data be encrypted. CDC has no mechanism in place to support non-CDC transfers. The sending and receiving sites must agree on the product that will be used for that purpose and identify the method of transfer. CDC will provide, upon request, the full version of the SEAL software; however, SEAL is a Java-based application that is executed within a DOS shell. SEAL does not have a graphical user interface (GUI). Many inexpensive, commercially available, easier to use, object-oriented software products are available for purchase. Additionally, a site may wish to consider the PHIN MS for point-to-point encryption and movement of data. For more details regarding PHIN MS, refer to the Web site <http://www.cdc.gov/phn/messaging>.

Access Control

Local Access

Requirement 26 Access to any surveillance information containing names for research purposes (that is, for other than routine surveillance purposes) must be contingent on a demonstrated need for the names, an Institutional Review Board (IRB) approval, and the signing of a confidentiality statement regarding rules of access and final disposition of the information. Access to surveillance data or information without names for research purposes beyond routine surveillance may still require IRB approval depending on the numbers and types of variables requested in accordance with local data release policies. (GP-1)

Most analyses of HIV/AIDS surveillance data do not require IRB approval; in fact, most such analyses do not require the inclusion of identifying information in the data sets. Occasionally, investigators from other health department units or academia want to conduct supplemental studies using reported case patients as their study population. Additionally, clinic-based researchers may want to obtain additional information on their patients. In these cases, the researcher should submit a request for the data set to

the HIV/AIDS surveillance coordinator. The surveillance coordinator should then refer to the local data release policy to determine if any of these types of data sets can be released. Data containing patients' names are not normally released for research purposes; further, the data release policy should anticipate that even data not containing names could be used to breach an individual's confidentiality if data sets are created or can be created that could indirectly identify any individual (e.g., a data set of all Asian hemophiliacs with AIDS in a county with a low Asian population and low morbidity).

Under certain circumstances and in accordance with local data release policies, the surveillance coordinator should refer the researcher to the Chair of the IRB. If the Chair determines that an IRB should be convened, both the researcher and surveillance coordinator must abide by the ruling. The IRB may approve the release of an analysis data set. Before a researcher obtains access to a data set, the surveillance coordinator must obtain a signed statement from the researcher certifying that he or she will comply with standards outlined in the local security policy. Signing this statement should indicate that the researcher (1) understands the penalties for unauthorized disclosure, (2) assures that the data will be stored in a secured area, and (3) agrees to sanitize or destroy any diskettes or other storage devices that contained the data set when the research project is completed. If the researcher is a member of the HIV/AIDS surveillance unit and already has a signed confidentiality statement on file, there is no need to sign an additional statement.

Under a signed assurance of confidentiality (see [Attachment D](#)), the HIV/AIDS surveillance information received by CDC that permits the identification of any individual is collected with a guarantee that it (1) will be held in strict confidence, (2) will be used only for purposes stated in the assurance, and (3) will not otherwise be disclosed or released without the consent of the individual in accordance with sections 306 and 308(d) of the Public Health Service Act.

Analysis databases or data sets that are released to individuals who work outside the secured area must be held securely until the data are approved for release. For example, health department epidemiologists or statisticians who do not work in the secured area often use analysis databases for routine analysis. The computers used in these circumstances must have protective software (e.g., user ID and password protection) to maintain data securely. Other robust authentication methods also may be used since the examples described are only the minimum required. Encryption software is not required with analysis databases because they are considered much less sensitive than those that contain names or other personal identifiers. Analysis data are still considered sensitive, since it may be possible to identify individuals by using particular combinations of reporting system variables. For that reason, analysis data should not be taken home, and all the results of all analyses performed by using reporting system variables must be approved for release as outlined in the surveillance unit's data release policy.

Requirement 27 Access to any secured areas that either contain surveillance data or can be used to access surveillance data by unauthorized individuals can only be granted during times when authorized surveillance or IT personnel are available for escort or under conditions where the data are protected by security measures specified in a written policy and approved by the ORP. (GP-1)

If unauthorized personnel (e.g., cleaning or maintenance crews) are allowed access to the secured area during times when surveillance staff are not present, then more stringent security measures must be employed inside the secured area to meet the program requirements. Under such circumstances, computerized surveillance information and data stored on one or more stand-alone computers or accessible via a LAN-connected workstation must be held securely with access controls in place, such as boot-up passwords that prevent unauthorized access to the computer's hard drive by booting from a system disk, encryption software, or storing the data on removable devices that can be locked away before allowing unauthorized personnel access. If surveillance information is stored on a LAN server, accounts with authorized access should be restricted by time of day and day of week. See [Requirement 7](#).

Managing keys or keypad codes to a secure area is difficult when personnel who receive the keys or codes are not directly supervised by the surveillance unit. Because of staff turnover in cleaning crews, the number of people who may be given keys or codes to the secure area may multiply over time. The more people with keys and codes, the greater the risk to the system. While tracking who has a key or code in this scenario can be difficult, it is recommended that a method of tracking and logging the issuance of keys or codes be implemented. It is further recommended that if an accurate accounting of all keys or codes to a secure area cannot be made, that the lock or code to that area be changed and issued using the tracking and logging method developed.

While many surveillance programs do not routinely grant access to the secured area to cleaning crews or maintenance staff, program requirements can be met even if cleaning crews are granted access without authorized escort, provided added measures (as discussed previously) are employed. The added measures must be named and described in the local security policy. For example, the policy might state that in lieu of escorting cleaning crews and other maintenance staff inside the secured area after hours, the surveillance unit will implement additional documented security measures to provide for enhanced data protection.

Requirement 28 Access to confidential surveillance information and data by personnel outside the surveillance unit must be limited to those authorized based on an expressed and justifiable public health need, must not compromise or impede surveillance activities, must not affect the public perception of confidentiality of the surveillance system, and must be approved by the ORP. (GP-1)

The primary function of HIV/AIDS surveillance is the collection and dissemination of accurate and timely epidemiologic data. Areas that elect to establish linkages to other public health programs for prevention or case management should develop policies

and procedures for sharing and using reported data that ensure the quality and security of the surveillance system. These programs should be developed in consultation with providers and community partners, such as their prevention planning groups. Recipients of surveillance information must be subject to the same training requirements and penalties for unauthorized disclosure as surveillance personnel.

Before establishing any program's linkage to confidential surveillance data, public health officials should define the public health objectives of the linkage, propose methods for the exchange of information, specify the type of surveillance data to be used, estimate the number of persons to be served by the linkage based on the availability of resources, outline security and confidentiality procedures, and compare the acceptability and effectiveness of basing the prevention programs on individual HIV/AIDS surveillance case reports to other strategies. The ORP must have the final approval of proposed linkages, since the ORP is ultimately responsible for any breach of confidentiality.

Prevention programs that use individual HIV/AIDS surveillance case data should evaluate the effectiveness of this public health approach. On an ongoing basis, programs also should assess confidentiality policies, security practices, and any breaches of confidentiality. Individual HIV/AIDS case reports should not be shared with programs that do not have well-defined public health objectives or with programs that cannot guarantee confidentiality.

Requirement 29 Access to surveillance information with identifiers by those who maintain other disease data stores must be limited to those for whom the ORP has weighed the benefits and risks of allowing access and can certify that the level of security established is equivalent to the standards described in this document. (GP-2)

Security is compromised if other programs that lack adequate standards to protect the security and confidentiality of the data are granted access to HIV/AIDS surveillance data or information and use that access to add HIV/AIDS data to their systems.

Linking records from the surveillance data with records from other databases semiannually or annually is encouraged to identify cases not previously reported, such as cases identified through TB surveillance or cancer surveillance. This provides a systematic means to evaluate the performance of health department surveillance and to take action to strengthen weaknesses in systems as they are identified. For example, programs can plan site visits with those providers who do not comply with state reporting laws to stimulate more timely and complete reporting.

Before the linkage of surveillance data, protocols should be discussed and developed. The protocol should address how the linkage will be performed using methods that are secure, who will analyze the results, and how the information will be used to improve the selected surveillance systems.

Requirement 30 Access to surveillance information or data for non-public health purposes, such as litigation, discovery, or court order, must be granted only to the extent required by law. (GP-2)

Some state laws mandate access to HIV/AIDS surveillance information for purposes other than law enforcement or litigation activities. For example, some states require school officials or prospective parents to be notified when they enroll or adopt HIV-infected children. However, the surveillance unit is not necessarily required to release the information just because it is requested by law enforcement or other officials. Access should be granted only to the extent required by law and not beyond any such requirement.

Any request for surveillance information for law enforcement purposes should be reviewed by the ORP with the appropriate program area's legal counsel to determine what specific information, if any, must be released from records maintained solely for epidemiologic purposes. Medical information may be available to the courts from less convenient but more appropriate sources. When information is ordered released as part of a judicial proceeding, any release or discussion of information should occur in closed judicial proceedings, if possible.

Central, Decentral, and Remote Access

The most secure protection for HIV/AIDS surveillance data is having only one centralized database in each state. Centralized data stores are those in which all electronic records of HIV/AIDS cases are stored in only one location within each state. Although not a program requirement, all states currently using the electronic reporting system in more than one location are strongly encouraged to move toward centralized operations where the electronic reporting system is deployed. As new software systems are deployed, CDC will provide technical and financial assistance to facilitate this transition.

Centralization of HIV/AIDS surveillance data within a state has clear benefits. First, centralized data stores offer greater security. Although having several HIV/AIDS surveillance databases throughout a state may have offered advantages in the past, those advantages may be outweighed by the risk of a security breach. Without centralization, most local jurisdictions must either mail copies of case reports to the state or mail external storage devices. Security risks are associated with both methods of data movement.

Centralized data stores add efficiency by improving case matching. With a centralized database, remote surveillance staff may conduct matches against the statewide database, thereby reducing intrastate duplicates and minimizing unnecessary field investigations of cases already reported elsewhere in the state.

Centralized systems may cost less to maintain. States with HIV/AIDS data systems in multiple locations must devote resources for providing technical assistance to surveillance staff at satellite locations. Finally, a centralized platform may support parallel surveillance systems (e.g., TB and STD). In other words, the hardware used for centralized systems could enhance surveillance activities for other diseases without increasing access to the HIV/AIDS database or compromising existing database security in any way.

Technologies such as browser-based applications, the Internet, Wide-Area Networks (WANs), and advances in data encryption technology and firewalls have made centralization of HIV/AIDS surveillance data more feasible.

New browser-based applications have numerous technical access controls, including authentication of the individual attempting access, assignment/restriction of access rights at the variable/field level, and assignment/restriction of access to functional components (role-based privileges). Use of a centralized database allows data entry and data analysis directly from the remote location while preventing access to non-authorized uses. Further, the capacity exists to assign access rights and privileges to staff just as is done in a decentralized system. In addition to these access controls, centralized systems can be configured to limit access by allowing only those connections originating from an authorized person using an authorized workstation.

A centralized database can be accessed using a WAN or the Internet, both of which have advantages and disadvantages. A WAN often uses transmission facilities provided by common carriers, such as telephone companies to establish a dedicated, private, and permanent point-to-point connection between satellite or remote offices and the central database, an option that may be cost-prohibitive for some states. All communications between points must still be password protected, and communications must be encrypted using methods that meet the data encryption standards set forth in this guidance.

Use of the Internet does not require dedicated phone lines and establishes temporary point-to-point connections over a public medium. This would be a less expensive alternative but, because the Internet is a public medium, a Virtual Private Network (VPN) must be established to guard against intrusion during communications. In addition to establishing a VPN, these communications must also be encrypted using methods that meet the data encryption standards set forth in this guidance. Additionally, firewalls must be in place to prevent unauthorized access.

When properly configured, a centralized system allows each local jurisdiction complete access to their HIV/AIDS data while prohibiting access by outside jurisdictions. A local jurisdiction can conduct local-level data analyses directly from a central dataset, or they may download a de-identified dataset for analysis.

If centralization is not yet feasible, each satellite site should maintain only cases within their jurisdiction. For matching case notifications, sites may consider the utility of maintaining limited data on out-of-jurisdiction cases receiving care and/or reported in their jurisdiction. Further, states are encouraged to consider limiting, as much as possible, the number of satellite locations.

Security Breaches

Requirement 31 All staff who are authorized to access surveillance data must be responsible for reporting suspected security breaches. Training of nonsurveillance staff must also include this directive. (GP-3)

Requirement 32 A breach of confidentiality must be immediately investigated to assess causes and implement remedies. (GP-4)

Requirement 33 A breach that results in the release of private information about one or more individuals (breach of confidentiality) should be reported immediately to the Team Leader of the Reporting, Analysis, and Evaluation Team, HIV Incidence and Case Surveillance Branch, DHAP, NCHSTP, CDC. CDC may be able to assist the surveillance unit dealing with the breach. In consultation with appropriate legal counsel, surveillance staff should determine whether a breach warrants reporting to law enforcement agencies. (GP-4)

A breach may be attempted, in progress, done without negative outcome, or done with negative outcome. Attention should be paid to identifying a breach, responding to it, repairing damage, learning from the event, and if necessary revising or enhancing policies and procedures, revising or instituting training, or enhancing physical or operational security.

By keeping a log of breaches and lessons learned from investigating them, the surveillance unit will be able to detect patterns of breaches, track compliance, and incorporate improvements to the security system.

After a breach has been detected, surveillance employees should notify their supervisor who may, depending on the severity of the breach, notify the ORP. Not all security breaches should be reported to CDC. Breaches that do not result in the unauthorized release of private information may be handled at the local/state health department level. However, CDC should be notified of all breaches of confidentiality (i.e., those breaches that result in the unauthorized disclosure of private information with or without harm to one or more individuals). If notified promptly, CDC may be able to provide assistance in responding to the breach in time to avert additional complications both in the state where the breach occurred and in other states. Notification also will allow CDC and the state to give consistent messages when contacted by the media.

Laptops and Portable Devices

Requirement 34 Laptops and other portable devices (e.g., personal digital assistants [PDAs], other hand-held devices, and tablet personal computers [PCs]) that receive or store surveillance information with personal identifiers must incorporate the use of encryption software. Surveillance information with identifiers must be encrypted and stored on an external storage device or on the laptop's removable hard drive. The external storage device or hard drive containing the data must be separated from the laptop and held securely when not in use. The decryption key must not be on the laptop. Other portable devices without removable or external storage components must employ the use of encryption software that meets federal standards. (GP-1)

Laptop computers, PDAs, and other hand-held or portable devices are becoming common tools for HIV/AIDS surveillance and may be key components of centralized surveillance systems. Unfortunately, laptops are vulnerable to theft. Although the likely target of the theft would be the device rather than the data, extreme care must be taken if the device stores HIV/AIDS surveillance data or information. If surveillance data are stored on the device's hard drive, hard drives must be removable and stored

separately when the device is being transported to and from the secured area. Alternatively, a security package that uses both software and hardware protection can be used. For example, an acceptable, though not as robust, level of protection can be achieved by using a smart disk procedure. This procedure prevents the device from booting up unless an encoded smart disk is inserted when the device is first turned on and a password is entered. Such a smart disk must not be stored with the device while in transit. The smart disk must be used in conjunction with an encryption package. Using this kind of protection scheme is critical because the device is capable of containing large amounts of sensitive information (e.g., names, addresses, dates of birth). Therefore, if a device has sensitive data on either an external storage device or hard drive, it must be taken back to the secured area at the close of business (unless out of town business travel is approved). Contingency plans should be in place that outline protective steps to take in case returning to the secure surveillance area is not possible. See [Requirement 24](#) and [Requirement 25](#). A removable drive is worth using even if data are encrypted and the laptop employs several layers of security.

Another option to consider when using laptops is to store encrypted data on an external storage device. If the device is lost or stolen, the data are protected. Unlike the laptop's hard drive, an external storage device lacks market value and is not as likely to be stolen or reused. Nonetheless, external storage devices containing patient identifiers must be encrypted when taken out of a secure area. For more information about removable and external storage devices, refer to section [Removable and External Storage Devices](#).

With the inception of Wireless Fidelity (Wi-Fi) products, many devices can now connect wirelessly to the Internet or a LAN. This functionality introduces risks regarding devices used to collect or store surveillance data. If these devices are not properly configured, data can be transmitted wirelessly over great distances without protection; this can result in the data being exposed to anyone with similar wireless products. Even if data are not being transmitted wirelessly but the device is capable of a wireless connection to the Internet, data stored on the device are susceptible to compromise by exposure to the Internet. For example, surveillance data may be collected in the field and stored on a laptop with Wi-Fi capability. The person collecting the data stops by a store that has a "hot spot" in order to connect to the Internet and check e-mail. The data stored on the laptop have the potential to be compromised. Any use of Wi-Fi or similar evolving wireless technologies must be given serious consideration when developing local policies. CDC strongly recommends that any local policy developed in response to Requirement 34 include explicit language regarding wireless technologies.

Removable and External Storage Devices

Requirement 35 All removable or external storage devices containing surveillance information that contains personal identifiers must

- (1) include only the minimum amount of information necessary to accomplish assigned tasks as determined by the surveillance coordinator,**
- (2) be encrypted or stored under lock and key when not in use, and**
- (3) with the exception of devices used for backups, devices should be sanitized immediately following a given task.**

External storage devices include but are not limited to diskettes, CD-ROMs, USB port flash drives (memory sticks), zip disks, tapes, smart cards, and removable hard drives. Deleting electronic documents does not necessarily make them irretrievable.

Documents thought to be deleted often are preserved in other locations on the computer's hard drive and on backup systems. Acceptable methods of sanitizing diskettes and other storage devices that previously contained sensitive data include overwriting or degaussing (demagnetizing) before reuse. Alternatively, the diskettes and other storage devices may be physically destroyed (e.g., by incineration). Such physical destruction would include the device, not just the plastic case around the device.

Attachment A

Additional Laptop Security Considerations

Basic Security

Choose a secure operating system and lock it down

An operating system that is secure and offers a secure logon, file level security, and the ability to encrypt data should be used. A password is considered a single-factor authentication process, but for enhanced security, commercial products can be used that change the access to a two-factor authentication. This can be achieved, for example, by using a password and an external device that must be plugged into the USB port. If such a device is used, it should meet federal standards.

Enable a strong BIOS password

The basic input/output system (BIOS) can be password protected. Some laptop manufacturers have stronger BIOS protection schemes than others. In some models, the BIOS password locks the hard drive so it cannot be removed and reinstalled into a similar machine.

Asset tag or engrave the laptop

Permanently marking (or engraving) the outer case of the laptop with a contact name, address, and phone number may greatly increase the likelihood of it being returned if it is recovered by the authorities. A number of metal tamper-resistant commercial asset tags are also available that could help the police return the hardware if it is recovered. Clearly marking the laptops may deter casual thieves.

Register the laptop with the manufacturer

Registering the laptop with the manufacturer will flag it if a thief ever sends the laptop in for maintenance. The laptop's serial number should be stored in a safe place. In the event the laptop is recovered, the police can contact you if they can trace it back to your office.

Physical Security

Get a cable lock and use it

Over 80% of the laptops on the market are equipped with a Universal Security Slot (USS) that allows them to be attached to a cable lock or laptop alarm. While this may not stop determined hotel thieves with bolt cutters, it will effectively deter casual thieves who may take advantage of users while their attention is diverted. Most of these devices cost between \$30 and \$50 and can be found at office supply stores or online. However, these locks only work if tethered properly to a strong, immovable, and unbreakable object.

Use a docking station

Many laptop thefts occur in the office. A docking station that is permanently affixed to the desktop and has a feature that locks the laptop securely in place can help prevent office theft. If a user is leaving the laptop overnight or for the weekend, a secure filing cabinet in a locked office is recommended.

Lock up the PCMCIA NIC cards

While locking the laptop to a desk with a cable lock may prevent laptop theft, a user can do little to keep someone from stealing the Personal Computer Memory Card International Association (PCMCIA) Network Interface Card (NIC) or modem that is inserted into the side of the machine. These cards can be removed from the laptop bay and locked in a secure location when not in use.

Use a personal firewall on the laptop

Once users connect to the Web from home or a hotel room, their data are vulnerable to attack, as firewall protection provided in the office is no longer available. Personal firewalls are an effective and inexpensive layer of security that can be easily installed. It is recommended that a third-party personal firewall be used to secure workstations.

Consider other devices based on needs

Since laptop use has become common, as has laptop theft, a variety of security-enhancing devices are now available. Motion detectors and alarms are popular items, as are hard drive locks. Biometric identification systems are also being installed on some laptop models, which allow the fingerprint to be the logon ID instead of a password. Cost, utility, and risk need to be taken into account when considering additional devices.

Preventing Laptop Theft

No place is safe

Precautions need to be taken with a laptop regardless of location, as no situation is entirely without risk. As discussed previously, the laptop should always be secured by using a cable lock or secure docking station.

Use a nondescript carrying case

Persons walking around a public place with a leather laptop case can be a target. A form-fitting padded sleeve for the laptop carried in a backpack, courier bag, briefcase, or other common nondescript carrying case may be safer. If a person is traveling in airports and train stations, small locks on the zippers of the case (especially backpacks) can be used (when not passing through security checkpoints) to prevent a thief from reaching into the bag.

Beware of distractions

Business travelers often use cell or pay phones in airports, restaurants, and hotel lobbies. Care needs to be taken that a laptop set down on the floor or a nearby table is not stolen while someone is engrossed in a telephone conversation.

When traveling by air

Sophisticated criminals can prey on travelers. When carrying a laptop, travelers need to use caution to safeguard it. When a person sets a laptop bag down for a minute to attend to other things, there may be a risk of theft. Always be aware of your surroundings because a thief could be waiting for that moment of distraction to grab a laptop (or other valuables).

When traveling by car

When transporting a laptop, it is safer to rent a car with a locking trunk (not a hatchback/minivan/SUV). Regardless of vehicle type, laptops should never be visible from outside of the car. Even when the laptop is in the trunk, the cable lock can be used to secure the laptop to the trunk lid so it cannot be taken easily.

While staying in a hotel

The hazards of leaving valuables in hotel rooms are well documented, and professional thieves know that many business travelers have laptops that can be resold. If a user keeps the laptop in the hotel room, it can be securely anchored to a metal post or fixed object.

Make security a habit

People are the weakest link in the security chain. If a person cares about the laptop and the data, a constant awareness of potential risks will help keep it safe. The laptop should always be locked up when it is not being used or is in storage. (A cable lock takes less time to install than it does for the PC to boot.) Use common sense when traveling and maintain physical contact with the laptop at all times. If a person is traveling with trusted friends or business associates, take advantage of the buddy system to watch each other's equipment.

Protecting Sensitive Data

Use the New Technology File System (NTFS) (proprietary to Windows operating systems)

Assuming a user has Windows NT/2000/XP on the laptop, use the NTFS to protect the data from laptop thieves who may try to access the data. File Allocation Table (FAT) and FAT32 file systems do not support file-level security and provide hackers with an opening into the system.

Disable the guest account

Always double check to make sure the guest account is not enabled. For additional security, assign a complex password to the account and completely restrict logon times. Some operating systems disable the guest account by default.

Rename the administrator account

Renaming the administrator account will stop some hackers and will at least slow down the more determined ones. If the account is renamed, the word 'Admin' should not be in the name. Use something innocuous that does not sound like it has rights to anything. Some computer experts argue that renaming the account will not stop everyone, because some persons will use the Security Identifier (SID) to find the name of the account and hack into it. The SID is a machine-generated, nonreadable binary string that uniquely identifies the user or group.

Consider creating a dummy administrator account

Another strategy is to create a local account named 'Administrator'; then give that account no privileges and a complicated 10+ digit complex password. If a dummy administrator account is created, enable auditing so a user knows when someone has tampered with it.

Prevent the last logged-in user name from being displayed

When a user presses **CTRL+ALT+DEL**, a login dialog box may appear that displays the name of the last user who logged into the computer. This can make it easier to discover a user name that can later be used in a password-guessing attack. This action can be disabled by using the security templates provided on the installation CD-ROM or via Group Policy snap-in. For more information, see Microsoft KB Article Q310125.

Enable EFS (Encrypting File System) in Windows operating systems

Some operating systems ship with a powerful encryption system that adds an extra layer of security for drives, folders, or files. This will help prevent a hacker from accessing the files by physically mounting the hard drive on another PC and taking ownership of files. Be sure to enable encryption on folders, not just files. All files that are placed in that folder will automatically be encrypted.

Disable the infrared port on a user laptop (if so equipped)

Some laptops transmit data via the infrared port on the laptop. It is possible for a person to browse someone else's files by reading the output from the infrared port without the laptop user knowing it. Disable the infrared port via the BIOS, or, as a temporary solution, simply cover it up with a small piece of black electrical tape.

Back up the data before a user leaves

Many organizations have learned that the data on the computer is more valuable than the hardware. Always back up the data on the laptop before a user does any extended traveling that may put the data at risk. This step does not have to take a lot of time, and a user can use the built-in backup utilities that come with the operating system. If the network does not have the disk space to back up all of the traveling laptop user's data, consider personal backup solutions including external hard drives (flash sticks), CD-Rs, and tape backup—all of which can also be encrypted.

Consider using offline storage for transporting sensitive data

Backing up the hard drive before users leave can help them retrieve the data when they return from a trip, but it does not provide an available backup of the data when they are out in the field. Several vendors offer inexpensive external storage solutions that can hold anywhere from 40 MB to 30 GB of data on a disk small enough to fit easily into the pocket. By having a backup of the files users need, they can work from another PC in the event that their laptop is damaged or missing. Most of these devices support password protection and data encryption, so the files will be safe even if a user misplaces the storage disk. When traveling, users should keep these devices with them, not in the laptop case or checked baggage. For additional security, lock or encrypt the files and have them sent by a courier service to the destination hotel or office.

Attachment B

Additional Security and Policy Considerations

Access and Storage Devices

Establish and implement policies and procedures for using and transporting secure access devices (smart card, key FOB, etc.) and external storage devices (diskettes, USB flash drives, CD-ROM, etc.).

Accountability

Maintain a record of the movements of hardware and electronic media and any persons responsible for transporting these devices.

Application and Data Criticality Analysis

Assess the relative criticality of specific applications and data in support of other contingency plan components.

Audit Controls and Logs

Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use protected electronic health information. Establish and implement policies and procedures that regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. Establish and implement policies and procedures for the backup, archiving, retention, and destruction of audit logs.

Automatic Logoff

Establish and implement policies and procedures that terminate any electronic session after a predetermined period of inactivity.

Browsers

Establish and implement policies and procedures regarding browser configuration for browser-based applications and Internet usage.

Certificates

Establish server and client digital certificate transportation, generation, and use policies.

Communications

Letterhead stationery, business cards, or dedicated phone lines are used among colleagues for professional purposes, and, in these cases, references to HIV/AIDS would not jeopardize the confidentiality of any case patient. In fact, such identification may be an important part of establishing credibility with providers who report cases. Addressing both purposes (protecting confidentiality and establishing credibility) will require careful organization and perhaps some duplication of communication mechanisms by surveillance

units (e.g., one card and phone line for investigation activities and another set for providers) or the use of more generic terminology (e.g., 'Epidemiology Unit' instead of 'HIV/AIDS Surveillance Unit').

Contingency of Operations and Disaster Recovery

Establish and implement policies and procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

A contingency planning policy and operations policy should address all critical aspects of contingency planning. Storage of data for backup and disaster recovery purposes should have the same if not more stringent accessibility, accountability, and encryption security requirements as a production system.

Along with the above, the following rules should be followed. They may be included in the policy or listed separately:

- Maintain list of all users and applications with access to the data. The list should include (per user or application) the day of week and the hours of the day that access will be needed. Access should be limited to these days and hours. The list should also identify those with access to identifiers.
- Conduct a monthly audit reflecting all successful/unsuccessful access. The report should include day, time of day, and length of access. It should be verified against authorized users and access requirements.
- Define administrative privileges for IT personnel (should be very limited). IT personnel need to have program approval before accessing the data.
- Identify some form of double authentication process for accessing the data.
- Keep systems containing the data in a secured area that is clearly labeled for authorized personnel only.
- Implement column and/or row level encryption of data.
- Create a data backup plan that includes procedures to create and maintain exact copies of protected electronic health information.
- Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity (time-outs).

Emergency Access Procedures

Establish and implement policies and procedures for obtaining necessary protected electronic health information during an emergency.

Emergency Mode Operation

Establish and implement policies and procedures to enable continuation of critical business processes for protecting the security of protected electronic health information while operating in emergency mode.

Encryption and Decryption

Implement a mechanism to encrypt and decrypt protected electronic health information.

Integrity Controls

Implement security measures to ensure that electronically transmitted protected electronic health information is not improperly modified without detection until disposed of. Ensure that any agent, including a contractor or subcontractor to whom it provides such information, agrees to implement reasonable and appropriate safeguards to protect the information.

Internet Connectivity

If a modem (internal or external), DSL, or cable is used on a workstation to provide access to the Internet, ensure that passwords and logon data used to access the Internet are not stored on the workstation. Most communications software has the capacity to dial a service and connect a user and even to send a password down the line. To prevent this from happening, never program a password into the workstation.

Some modems have the capability to answer the telephone as well as to make calls. Make sure users know how to tell if their modem has been placed in answering mode and how to turn off that mode. External modems normally have an indicator light labeled AA that glows if Auto Answer mode is selected. Internal modems are harder to monitor, but small utility programs are available that can help. Callback modems actually call the user back at a prearranged number. External modems are recommended because the ease of turning them off offers programs the greatest degree of control.

CDC highly recommends that workstations holding confidential and sensitive data that are connected to the Internet should be disconnected from the Internet except when the Internet is being used for authorized activities.

If the line is for data only, make sure that the telephone number of the line does not appear in the telephone directory and is not displayed on the telephone itself or on the wall socket.

Intrusion Detection

Establish and implement policies and procedures regarding intrusion detection and penetration vulnerabilities.

Keyboard and Screen Locking

Establish and implement policies and procedures for screen saving and keyboard locking.

Logins and Monitoring

Establish and implement policies and procedures for workstation logins, and designate who can request and authorize changes to a login. Establish and implement policies and procedures for monitoring login attempts and reporting discrepancies.

Maintenance Records

Establish and implement policies and procedures to document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, and locks).

Media Disposal and Re-use

Establish and implement policies and procedures to address the final disposition of protected electronic health information, and/or the hardware or electronic media on which it is stored. Establish and implement policies and procedures for removal of protected electronic health information from electronic media before the media are made available for re-use.

Networks, LANs, and WANs

Establish and implement policies and procedures governing all servers on the network. Establish and implement policies and procedures for the documentation of network configurations and architectures. Topics to include are

- Name and location of servers
- Netware protocols
- Users, groups, and roles that access data and physical server
- Authentication protocols
- e-mail hosting
- Remote access
- Web hosting
- Data located on each server
- Administrative safeguards

Computers used to maintain HIV/AIDS surveillance information with personal identifiers should not be connected to other computers or computer systems that are located outside of the secure area until and unless the connection is deemed secure by adding multiple layers of protective measures—including encryption software, restricted access rights, and physical protections for the LAN equipment and wiring—and justifying a public health need to maintain highly sensitive data on a system that has multiple users and multiple locations. This system should operate under a certified LAN administrator, who will attest to the system's effectiveness and assume responsibility for any breach of security directly resulting from the system's failure to protect sensitive data.

Internet access devices (e.g., modems and network interface cards) or cables should not be connected to any computer or computer system containing surveillance information and data unless authorized staff need Internet access as a means to enhance surveillance activities. If Internet connectivity is used for surveillance activities, specific rules of use should be provided in writing to authorized users, and they should sign a statement that they understand those rules.

Password Management

Establish and implement policies and procedures for creating, changing, and safeguarding passwords.

Patching and Service Packs

Establish and implement policies and procedures for security patching and service pack control.

Protection from Malicious Software

Establish and implement policies and procedures for guarding against, detecting, and reporting malicious software.

Risk Analysis

Establish and implement policies and procedures that require conducting a regular, accurate, and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of protected electronic health information held by the covered entity.

Routers and Firewalls

Establish and implement policies and procedures regarding router and firewall logs to capture packets that violate filter criteria. Establish and implement policies and procedures for firewall and router configuration.

Software Inventory, Releases, Licensing, and Upgrades

Establish and implement policies and procedures for the inventory of authorized software (including versions) that can be installed on development, training, testing, staging, and production servers and workstations.

Establish and implement policies and procedures for tracking and verifying software licenses.

Establish and implement policies and procedures for prerelease and testing of software. Establish a methodology to deploy new or upgraded software to all appropriate workstations and servers (configuration management). Establish a method for tracking the software loaded on every workstation and server.

Testing and Revision of Plans

Establish and implement policies and procedures for periodic testing and revision of contingency plans.

Transmission Security

Implement technical security measures to guard against unauthorized access to protected electronic health information that is being transmitted over an electronic communications network.

Workstation Use

Establish and implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access protected electronic health information.

Attachment C

Federal Encryption Standards

CDC Policy

Encryption is required when any moderately or highly sensitive files, any moderately or highly critical information, or any limited access/proprietary information is to be transmitted either electronically or physically.

Federal Standards

The National Institute of Standards and Technology (NIST) uses the Federal Information Processing Standards (FIPS) for the Advanced Encryption Standard (AES), FIPS-197. This standard specifies Rijndael as a FIPS-approved symmetric encryption algorithm that may be used by U.S. government organizations (and others) to protect sensitive information. Federal agencies should also refer to guidance from the Office of Management and Budget (OMB).

Advanced Encryption Standard (AES)

**Federal Information
Processing Standards Publication 197
November 26, 2001**

Name of Standard: Advanced Encryption Standard (AES) (FIPS PUB 197).

Category of Standard: Computer Security Standard, Cryptography.

Explanation: The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called cipher text; decrypting the cipher text converts the data back into its original form, called plaintext. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits.

Approving Authority: Secretary of Commerce.

Maintenance Agency: Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL).

Attachment D

CDC Assurance of Confidentiality

ASSURANCE OF CONFIDENTIALITY FOR SURVEILLANCE OF ACQUIRED IMMUNODEFICIENCY SYNDROME (AIDS) AND INFECTION WITH HUMAN IMMUNODEFICIENCY VIRUS (HIV) AND SURVEILLANCE-RELATED DATA (INCLUDING SURVEILLANCE INFORMATION, CASE INVESTIGATIONS AND SUPPLEMENTAL SURVEILLANCE PROJECTS, RESEARCH ACTIVITIES, AND EVALUATIONS)

The national surveillance program for HIV/AIDS is being coordinated by the Surveillance Branch of the Division of HIV/AIDS Prevention - Surveillance and Epidemiology (DHAP - SE), the National Center for HIV/STD/TB Prevention, a component of the Centers for Disease Control and Prevention (CDC), an agency of the United States Department of Health and Human Services. The surveillance information requested by CDC consists of reports of persons with suspected or confirmed AIDS or HIV infection, including children born to mothers infected with HIV, and reports of persons enrolled in studies designed to evaluate the surveillance program. The information collected by CDC is abstracted from laboratory, clinical, and other medical or public health records of suspected or confirmed HIV/AIDS cases; and from surveys that interview persons in recognized HIV risk groups or known to have a diagnosis of HIV/AIDS.

Surveillance data collection is conducted by State and Territorial health departments that forward information to CDC after deleting patient and physician names and other identifying or locating information. Records maintained by CDC are identified by computer-generated codes, patient date of birth, and a state/city assigned patient identification number. The data are used for statistical summaries and research by CDC scientists and cooperating state and local health officials to understand and control the spread of HIV/AIDS. In rare instances, expert CDC staff, at the invitation of state or local health departments, may participate in research or case investigations of unusual transmission circumstances or cases of potential threat to the public health. In these instances, CDC staff may collect and maintain information that could directly identify individuals.

Information collected by CDC under Section 306 of the Public Health Service Act (42 U.S.C. 242k) as part of the HIV/AIDS surveillance system that would permit direct or indirect identification of any individual or institution, on whom a record is maintained, and any identifiable information collected during the course of an investigation on either persons supplying the information or persons described in it, is collected with a guarantee that it will be held in confidence, will be used only for the purposes stated in this Assurance, and will not otherwise be disclosed or released without the consent of the individual or institution in accordance with Section 308 (d) of the Public Health Service Act (42 U.S.C. 242m(d)). This protection lasts forever, even after death.

Information that could be used to identify any individual or institution on whom a record is maintained by CDC will be kept confidential. Full names, addresses, social security numbers, and telephone numbers will not be reported to this national HIV/ AIDS surveillance system. Medical, personal, and lifestyle information about the individual, and a computer-generated patient code will be collected.

Surveillance information reported to CDC will be used without identifiers primarily for statistical and analytic summaries and for evaluations of the surveillance program in which no individual or institution on whom a record is maintained can be identified, and secondarily, for special research investigations of the characteristics of populations suspected or confirmed to be at increased risk for infection with HIV and of the natural history and epidemiology of HIV/AIDS. When necessary for confirming surveillance information or in the interest of public health and disease prevention, CDC may confirm information contained in case reports or may notify other medical personnel or health officials of such information; in each instance, only the minimum information necessary will be disclosed.

No CDC HIV/AIDS surveillance or research information that could be used to identify any individual or institution on whom a record is maintained, directly or indirectly, will be made available to anyone for non-public health purposes. In particular, such information will not be disclosed to the public; to family members; to parties involved in civil, criminal, or administrative litigation, or for commercial purposes; to agencies of the federal, state, or local government. Data will only be released to the public, to other components of CDC, or to agencies of the federal, state, or local government for public health purposes in accordance with the policies for data release established by the Council of State and Territorial Epidemiologists.

Information in this surveillance system will be kept confidential. Only authorized employees of DHAP - SE in the Surveillance Branch and Statistics and Data Management Branch, their contractors, guest researchers, fellows, visiting scientists, research interns and graduate students who participate in activities jointly approved by CDC and the sponsoring academic institution, and the like, will have access to the information. Authorized individuals are required to handle the information in accordance with procedures outlined in the Confidentiality Security Statement for Surveillance of Acquired Immunodeficiency Syndrome (AIDS) and Infection with Human Immunodeficiency Virus (HIV) and Surveillance-Related Data (Including Surveillance Information, Case Investigations and Supplemental Surveillance Projects, Research Activities, and Evaluations).

Attachment E

Sample Employee Oath - Texas

TEXAS DEPARTMENT OF HEALTH EMPLOYEE CONFIDENTIALITY AGREEMENT

BACKGROUND INFORMATION:

The Texas Department of Health (TDH) guiding principles establish the paramount importance of patient and client confidentiality in the mission of this department. Information in reports, records, correspondence, and other documents routinely dealt with by employees of the Texas Department of Health may be privileged, confidential, private, or a combination of two or more. In each instance, the information may receive its designation by statute or judicial decision. Such statutes as the *Open Records Act*, *Medical Practice Act*, and the *Communicable Disease Act* contain provisions, which make certain information that comes to TDH privileged and/or confidential.

As a general rule, in transactions carried out on a day-to-day basis, the Medical Practice Act makes medical records and information taken from medical records privileged and confidential. All communicable disease records (STD, HIV, and TB) are made confidential by the Communicable Disease Act. Birth and death records are confidential for 50 years through the provisions dealing with vital statistics in the Open Records Act and other laws. If information is "confidential," it is generally information that should be kept secret and is given only to another person who is in a position of trust. "Privileged" information protects a person who has either given or received confidential information from being revealed in a legal proceeding. Other information that contains "highly intimate or embarrassing facts about a person such that its disclosure 'would be highly offensive to a [reasonable] person...'" and is not of legitimate concern of the public or might hold a person up to the scorn or ridicule of his or her peers if made public, is made confidential by the common law doctrine of the right to privacy [ORD-262, 1980]. Statutes that govern the operation of the department may contain additional provisions that render information that comes into the hands of certain programs in the TDH privileged, confidential, and/or private.

Note to employee: If you have questions regarding confidentiality, you should contact your immediate supervisor or the Office of General Counsel. The signed Employee Confidentiality Agreement will be filed in your personnel folder.

AGREEMENT:

I agree that:

- A patient record or any information taken from a patient record is privileged and confidential. In most instances, such information may not be released unless the person identified in the record provides written consent, or the release of information is otherwise permitted by law. A patient record is defined as: a record of identity and diagnosis of a patient that is initiated and maintained by, or at the direction of a physician, dentist, or someone under the direction or protocols of a physician or dentist.
- I understand that I must not release information from reports, records, correspondence, and other documents, however acquired, containing medical or other confidential information, and that I may not release such information except in a manner authorized by law, such as in a statistical form that will not reveal the identity of an individual or with the written consent of the individual involved.
- I may not release or make public, except as provided by law, Individual case information including demographic data and client contacts.
- I will keep all confidential files, including computer diskettes, in a locked file cabinet when not in use.
- When I am working on a confidential file, I will "lock up" the information when I leave my workstation for lunch, meetings, or for the day. I understand that to "lock up" the information includes *logging off my computer*, not merely saving and closing the confidential file.
- I will keep any confidential files I work with out of the view of unauthorized persons.
- I will not discuss confidential information with people who are not authorized, and/or who do not have a need to know the information.
- When I work with files that contain personal identifiers, I will log off my computer when I am not actively using the file.
- I will conduct telephone conversations and/or conferences, that require the identification of patients by name, in secure areas where the conversation or conference will not be overheard or seen.
- To protect confidentiality, I will not discuss the facts contained in confidential documents in a social setting.
- When transporting information that is privileged, confidential, or private, I will employ appropriate security measures to ensure the material remains protected.

- I will keep information relating to the regulatory activities of the department confidential. Regulatory activities include at least the following: survey schedules, unannounced site visits, survey results, information pertaining to complaints that have been investigated, litigation information, and personnel actions.
- Where applicable, departmental policy requires that personnel have individual passwords to access confidential computer files. I will not use another person's password nor will I disclose my own.
- I understand that my superiors will document any violations of this agreement and he or she will place the documentation in my main personnel file maintained by the Bureau of Human Resources.
- If I am a professional employee (e.g. physician, registered nurse, attorneys, etc.) or I am an employee supervised by or providing support to a professional employee, I understand that I may be subject to additional rules of confidentiality. This agreement does not supersede the code of professional conduct and I further understand that a violation of the code of professional conduct may subject the professional employee to additional sanctions (e.g. loss of license.)
- When I dispose of a document that contains patient information, I will assure that the document is shredded.

I have read this Confidentiality Agreement and I understand its meaning. As an employee of the Texas Department of Health, I agree to abide by the Confidentiality Agreement. I further understand that should I improperly release or disclose privileged, confidential, or private information, I may be subject to an adverse personnel action, up to and including the termination of my employment. I understand that I may be subject to civil monetary penalties, criminal penalties or liability for money damages for such an action.

SIGNATURE:

Employee's Name: _____
Print Employee's Name Date

Employee's Signature: _____

Sample Employee Oath - Seattle/King County

*Public Health—Seattle & King County (PH-SKC)
Prevention Division—HIV/AIDS Epidemiology Unit*

Confidentiality Agreement

As a PH-SKC employee in the HIV/AIDS Epidemiology Unit, or as a subcontracted employee, student, visiting professional, or work study student, I understand that I may have access to confidential information on persons with reportable diseases, persons counseled during clinical or prevention activities, study participants, or clients of sites involved in our work. This information includes any surveillance- or study-related electronic or paper records or information given orally during an interview or counseling session or through other related contact (e.g., scheduling appointments or updating locators in person or on the phone). Information may also come from records of participating institutions and health care providers, medical/health clinics, drug treatment centers and jails. Examples of confidential information include but are not limited to names, addresses, telephone numbers, sexual and drug-use behaviors, medical, psychological and health-related conditions and treatment, religious beliefs, finances, living arrangements, and social history. **By signing this statement, I am indicating my understanding of my responsibilities and agree to the following:**

- I agree to uphold the confidentiality and security policies specific to my work site(s) and, if required by my work site protocol, to wear my badge that identifies me as a PH-SKC employee when conducting any research, surveillance or prevention activities at field sites outside the office.
- I agree not to divulge, publish, or otherwise make known to unauthorized persons or to the public any information obtained that could identify persons reported with notifiable diseases, persons served during the course of prevention or clinical activities, participants in research or evaluation studies or any information regarding the identity of any patient or client of any institution including any alcohol or drug treatment program to which I have access.
- I understand that all client, patient, and disease report information and records compiled, obtained, or accessed by me in the course of my work are confidential. I agree not to divulge or otherwise make known to unauthorized persons any information regarding the same, unless specifically authorized to do so by office protocol or by a supervisor acting in response to applicable law, court order, or public health or clinical need (WA Administrative Code 246-101-515).
- I understand that I am not to read information and records concerning patients, clients, or study participants, or any other confidential documents, nor ask questions of clients during interviews for my own personal information but only to the extent and for the purpose of performing my assigned duties.
- I understand that a breach of security or confidentiality may be grounds for disciplinary action by PH-SKC, and may include termination of employment.

HIV/AIDS Surveillance Guidelines — Security and Confidentiality

- I understand that the civil and criminal penalties set forth in the Revised Code of Washington (RCW 70.24.080 and 70.24.084) include, for each breach of STD/HIV records, a fine of \$1000 or actual damages for negligent violation and \$10,000 or actual damages for intentional or reckless violation, which I would be personally responsible for paying. Breach of other communicable disease records may result in civil penalties imposed by a court and include actual damages and attorneys' fees (RCW 70.02). Alcohol and drug abuse patient records are protected by federal law (42 CFR Part 2) with criminal penalties for violation.

- I understand that action to impose civil or criminal penalties against me may be taken by a prosecuting attorney or another party with standing if I am suspected of being responsible for a breach of confidentiality.

- I agree to notify my supervisor immediately should I become aware of an actual breach of confidentiality or a situation which could potentially result in a breach, whether this be on my part or on the part of another person.

Signature

Date

Printed name

Signature of Program Manager

Date

Printed name

Sample Employee Oath - Louisiana

**STATE OF LOUISIANA
DEPARTMENT OF HEALTH & HOSPITALS**

**Louisiana Office of Public Health
HIV/AIDS Program**

Confidentiality Agreement

As an HIV/AIDS Program employee, subcontracted employee, student, or visiting professional, I understand that I will be exposed to some very privileged patient information. Examples of such information are medical conditions, medical treatments, finances, living arrangements, and sexual orientation. The patient's right to privacy is not only a policy of the HIV/AIDS Program, but is specifically guaranteed by statute and by various governmental regulations.

I understand that intentional or involuntary violation of the confidentiality policies is subject to appropriate disciplinary action(s), that could include being discharged from my position and/or being subject to other penalties. By initialing the following statements I further agree that:

Initial below

_____ I will never discuss patient information with any person outside of the program who is not directly affiliated with the patient's care.

_____ If in the course of my work I encounter facilities or programs without strict confidentiality protocols, I will encourage the development of appropriate confidentiality policies and procedures.

_____ I will handle confidential data as discretely as possible and I will never leave confidential information in view of others unrelated to the specific activity. I will keep all confidential information in a locked cabinet when not in use. I will encrypt all computer files with personal identifiers when not in use.

_____ I will shred any document to be disposed of that contains personal identifiers. Electronic files will be permanently deleted, in accordance with current HAP required procedures, when no longer needed.

_____ I will maintain my computer protected by power on and screen saver passwords. I will not disclose my computer passwords to unauthorized persons.

_____ I understand that I am responsible for preventing unauthorized access to or use of my keys, passwords, and alarm codes.

_____ I understand that I am bound by these policies, even upon resignation, termination, or completion of my activities.

I agree to abide by the HIV/AIDS Program Confidentiality Policy. I have received, read, understand, and agree to comply with these guidelines.

Warning: Persons who reveal confidential information may be subject to legal action by the person about whom such information pertains.

Signature

Date

Printed Name

Supervisor's Signature

Date

Attachment F

Glossary of Surveillance and Technical Terms

Access: The ability or the means necessary to read, write, modify, or communicate data/information. To gain entry to memory in order to read or write data. The entrance to the Internet or other online service or network.

Access control: A cohesive set of procedures (including management, technical, physical, and personnel procedures) that are designed to assure to a given level of reliability that an individual:

- 1) is the person he or she claims to be (authentication),
- 2) has a verified public health need to have access to surveillance systems and information,
- 3) has been authorized to perform the action or access the data, and
- 4) is doing so from an authorized place using an authorized process.

ACL: Short for AccessControl List, ACL is a listing that tells a computer operating system or other network devices what rights a user has to each item on a computer or network device.

Adware: 1) (ADvertisementWARE) Software that periodically pops up ads in a user's computer. Adware is considered spyware and is installed without the user's knowledge. It typically displays targeted ads based on words searched for on the Web or derived from the user's surfing habits that have been periodically sent in the background to a spyware Web server. 2) (AD supported softWARE) Software that is given away because it contains advertising messages.

Aggregated data: Information, usually summary statistics, that may be compiled from personal information, but is grouped in a manner to preclude the identification of individual cases. An example of properly aggregated data might be, 'Whiteacre County reported 1,234 cases of AIDS during 1997 among Hispanics.' An example of improperly aggregated data might be, 'Blackacre County reported 1,234 cases of AIDS during 1997 among Hispanics and 1 case among American Indians.'

Analysis data, datasets, or database: A dataset created by removing personal data (e.g., names, addresses, ZIP codes, and telephone numbers) so the record or records cannot be linked to an individual, but still allows the remaining data to be analyzed.

Antivirus program: A software program designed to protect a computer and/or network against computer viruses. When a virus is detected, the computer will generally prompt the user that a virus has been detected and recommend an action such as deleting the virus.

Authentication: Verifying the identity of a user who is logging onto a computer system or verifying the origin of a transmitted message. Authentication depends on four classes of data, generally summarized as 'what you know,' 'what you have,' 'what you are,' and 'what you do.'

Authorized access: As determined by the ORP or a designee, the permission granted to individuals to see full or partial HIV/AIDS surveillance information and data that potentially could be identifying or linked to an individual. The ORP or designee should make these determinations according to role-based (or need-to-know) responsibilities.

Authorized personnel: Those individuals employed by the program who, in order to carry out their assigned duties, have been granted access to confidential HIV/AIDS surveillance information. Authorized personnel must have a current, signed, approved, and binding nondisclosure agreement on file.

Availability: The accessibility of a system resource in a timely manner; for example, the measurement of a system's uptime. Availability is one of the six fundamental components of information security.

Biometrics: The biological identification of a person, which includes characteristics of structure and of action such as iris and retinal patterns, hand geometry, fingerprints, voice responses to challenges, and the dynamics of handwritten signatures. Biometrics are a more secure form of authentication than typing passwords or even using smart cards, which can be stolen; however, some forms have relatively high failure rates. Biometric authentication is often a secondary mechanism in two-factor authentication.

Biometric signature: The characteristics of a person's handwritten signature. The pen pressure and duration of the signing process, which is done on a digital-based pen tablet, is recorded as an algorithm that is compared against future signatures.

BIOS (basic input/output system): The built-in software that determines what a computer can do without accessing programs from a disk. On personal computers, the BIOS contains all the code required to control the keyboard, display screen, disk drives, serial communications, and a number of miscellaneous functions.

The BIOS is typically placed in a Read-Only Memory (ROM) chip that comes with the computer (it is often called a ROM BIOS). This ensures that the BIOS will always be available and will not be damaged by disk failures. It also makes it possible for a computer to boot itself. Because Random-Access Memory (RAM) is faster than ROM, many computer manufacturers design systems so that the BIOS is copied from ROM to RAM each time the computer is booted. This is known as shadowing. Many modern PCs have flash BIOS, which means that the BIOS has been recorded on a flash memory chip, which can be updated if necessary.

Breach: A breach is a condition of departure from established policies or procedures. A breach can only be understood in view of a written reference point that describes the desired condition and the link between that condition and the surveillance objectives associated with maintaining the condition. A breach is an infraction or violation of a standard, obligation, or law. A breach in data security would include any unauthorized use of data, even data without names. A breach, in its broadest sense, may be caused by an act of God, a person, or an application/system and may be malicious in nature or purely unintended. An example of a malicious breach would be if staff intentionally, but without authorization, released patient names to the public. An example of an unintended breach would be if completed HIV/AIDS case reports were inadvertently mailed to and read by an unauthorized individual. A breach does not necessarily mean that sensitive information was released to the public or that any one person was harmed. A minor infraction, like forgetting to lock a file drawer containing sensitive information (even if inside a secure area), constitutes a breach of security protocol as compared with a breach of confidentiality.

Other examples of possible breaches:

- 1) A hacker gains access to an internal machine via the Internet or a dial-up connection.
- 2) A trusted programmer introduces a program into the production environment that does not behave within expected limits.
- 3) A technician creates a backdoor into the operation of a system, even for positive and beneficial reasons, that alters the information protection provided.
- 4) After having been entered into a computerized file, confidential forms are left for removal in the standard paper waste process in an openly accessible location.

Breach of confidentiality: A security infraction that results in the release of private information with or without harm to one or more individuals.

Case-specific information: Any combination of data elements that could identify a person reported to the surveillance system. An example of case-specific information without a name might be, 'A woman with hemophilia from Whiteacre County was diagnosed with AIDS in 1997.'

Certificate: See Digital certificate.

Certification authority or certificate authority: An organization that issues digital certificates (digital IDs) and makes its public key widely available to its intended audience.

Checksum: A value used to ensure data are stored or transmitted without error. It is created by calculating the binary values in a block of data using some algorithm and storing the results with the data. When the data are retrieved from memory or received at the other end of a network, a new checksum is computed and matched against the existing checksum. A nonmatch indicates an error. Just as a check digit tests the accuracy of a single number, a checksum tests a block of data. Checksums detect single bit errors and some multiple bit errors, but are not as effective as the Classes, Responsibilities, and Collaborations (CRC) design method. Checksums are also used by the Sophos antivirus software to determine if a file has changed since the last time it was scanned for a virus.

Ciphertext: Data that have been coded (enciphered, encrypted, encoded) for security purposes. Contrast with plaintext and cleartext.

CISSP: The Certified Information Systems Security Professional (CISSP) exam is designed to ensure that someone handling computer security for an organization or client has mastered a standardized body of knowledge. The certification was developed and is maintained by the International Information Systems Security Certification Consortium (ISC²). The exam certifies security professionals in 10 different areas:

- 1) Access control systems and methodology
- 2) Application and systems development security
- 3) Business continuity planning & disaster recovery planning
- 4) Cryptography
- 5) Law, investigation, and ethics
- 6) Operations security
- 7) Physical security
- 8) Security architecture and models
- 9) Security management practices
- 10) Telecommunications and networking security

Cleartext: Same as plaintext.

Confidential information: Any information about an identifiable person or establishment, when the person or establishment providing the data or described in it has not given consent to make that information public and was assured confidentiality when the information was provided.

Confidentiality: The protection of private information collected by the surveillance system.

Confidential record: A record containing private information about an individual or establishment.

Cookies: Data created by a Web server that are stored on a user's computer either temporarily for that session only or permanently on the hard disk (persistent cookie). Cookies provide a way for the Web site to identify users and keep track of their preferences. They are commonly used to maintain the state of the session. The cookies contain a range of Uniform Resource Locators (URLs, or addresses) for which they are valid. When the Web browser or other Hypertext Transfer Protocol (HTTP) application sends a request to a Web server with those URLs again, it also sends along the related cookies. For example, if the user ID and password are stored in a cookie, it saves the user from typing in the same information all over again when accessing that service the next time. By retaining user history, cookies allow the Web site to tailor the pages and create a custom experience for that individual. A lot of personal data reside in the cookie files on the computer. As a result, this storehouse of private information is sometimes the object of attack. A browser can be configured to prevent cookies, but turning them off entirely can limit the Web features. Browser settings typically default to allowing first party cookies, which are generally safe because they are only sent back to the Web site that created them. Third party cookies are risky because they are sent back to sites other than the one that created them. To change settings, look for the cookie options in the Options or Preferences menu within the browser.

Cookie poisoning: The modification of or theft of a cookie in a user's machine by an attacker in order to release personal information. Cookies that log onto password-protected Web sites automatically send username and password. Thieves can thus use their own computers and confiscated cookies to enter victims' accounts.

Cryptography: The conversion of data into a secret code for transmission over a public network. The original text or plaintext is converted into a coded equivalent called ciphertext via an encryption algorithm. The ciphertext is decoded (decrypted) at the receiving end and turned back into plaintext. The encryption algorithm uses a key, which is a binary number that is typically from 40 to 256 bits in length. The greater the number of bits in the key (cipher strength), the more possible key combinations and the longer it would take to break the code. The data are encrypted or locked by combining the bits in the key mathematically with the data bits. At the receiving end, the key is used to unlock the code and restore the original data.

Cryptographic key: A numeric code that is used to encrypt text for security purposes.

Data stewards: Refers to individuals responsible for the creation of the data used or stored in organizational computer systems. The data steward determines the appropriate sensitivity and classification level and reviews that level regularly for appropriateness. The data stewards have final responsibility for protecting the information assets and are responsible for ensuring the information assets under their control adhere to local policies. The data steward is one or more of the following:

- 1) The creator of the information
- 2) The manager of the creator of the information
- 3) The receiver of external information
- 4) The manager of the receiver of the external information

Data user: Anyone who routinely uses the data. Data users are responsible for following operating procedures, taking due care to protect information assets they use, and using computing resources of the department for department purposes only.

Denial of service (DoS): A DoS attack is a form of attacking another computer or organization by sending millions or more requests every second causing the network to slow down, cause errors, or shut down. Because it is difficult for a single individual to generate a DoS attack, these forms of attacks are often created by another organization and/or worms that in turn create zombie computers to create a DoS attack.

DES (Data Encryption Standard): An algorithm that encrypts and decrypts data in 64-bit blocks, using a 64-bit key (although the effective key strength is only 56 bits). It takes a 64-bit block of plaintext as input and outputs a 64-bit block of ciphertext. Since it always operates on blocks of equal size and it uses both permutations and substitutions in the algorithm, DES is both a block cipher and a product cipher.

Digital certificate: The digital equivalent of an ID card used in conjunction with a public key encryption system. Also called digital IDs, digital certificates are issued by a trusted third party known as a certification authority or certificate authority (CA) such as VeriSign, Inc. (www.verisign.com). The CA verifies that a public key belongs to a specific organization or individual, and the certification process varies depending on the level of certification and the CA itself. Driver's licenses, notarization, and fingerprints are types of documentation that may be used. The digital certificate typically uses the X.509 file format and contains CA and user information, including the user's public key (details below). The CA signs the certificate by creating a digest, or hash, of all the fields in the certificate and encrypting the hash value with its private key. The signature is placed in the certificate. The process of verifying the signed certificate is done by the recipient's software such as a Web browser or e-mail program. The software uses the widely known public key of the CA to decrypt the signature back into the hash value. If the decryption is successful, the identity of the user is verified. The software then recomputes the hash from the raw data (cleartext) in the certificate and matches it against the decrypted hash. If they match, the integrity of the certificate is verified (it was not tampered with). A signed certificate (the digital certificate) is typically combined with a signed message, in which case the signature in the certificate verifies the identity of the user while the signature in the message verifies the integrity of the message contents. The fact that the message is encrypted ensures privacy of the content. The CA keeps its private key very secure, because if it were ever discovered, false certificates could be created.

Digital signature: A digital guarantee that a file has not been altered, as if it were carried in an electronically sealed envelope. The signature is an encrypted digest (one-way hash function) of the text message, executable or other file. The recipient decrypts the digest that was sent and recomputes the digest from the received file. If the digest matches the file, it is proven to be intact and tamper free as received from the sender.

Disaster recovery: A plan for duplicating computer operations after a catastrophe occurs, such as a fire or earthquake. It includes routine off-site backup as well as a procedure for activating necessary information systems in a new location. The ability to recover information systems quickly after the terrorist attacks of 9/11 proved the value of disaster recovery. Many companies that had programs in place were up and running within a few days in new locations. Companies that did not have disaster recovery systems in place have had the most difficulty recreating their information infrastructure.

Distributed denial of service: On the Internet, a distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users. A hacker (or cracker) begins a DDoS attack by exploiting vulnerabilities in one computer system and making it the DDoS master. It is from the master system that the intruder identifies and communicates with other systems that can be compromised. The intruder loads cracking tools available on the Internet on multiple (sometimes thousands of) compromised systems. With a single command, the intruder instructs the controlled machines to launch one of many flood attacks against a specified target. The inundation of packets to the target causes a denial of service. While the press tends to focus on the target of DDoS attacks as the victim, in reality there are many victims in a DDoS attack including the final target and the systems controlled by the intruder.

Encryption: Encryption is defined as the manipulation or encoding of information so that only parties intended to view the information can do so. There are many ways to encrypt information, and the most commonly available systems involve public key and symmetric key cryptography. A public key system uses a mathematically paired set of keys, a public key and a private key. Information encrypted with a public key can only be decrypted with the corresponding private key, and vice versa. Therefore, you can safely publish the public key, allowing anyone to encrypt a message that can be read only by the holder of the private key. Presuming that the private key is known to only one authorized individual, the message is then accessible only to that one individual. A symmetric key system is based on a single private key that is shared between parties. Symmetric systems require that keys be transmitted and held securely in order to be effective, but are considered to be highly effective when the procedures are good and the number of individuals who possess the key is small. In general, under both systems, the larger the key, the more robust the protection.

Encrypting File System (EFS): A feature of the Windows 2000 operating system (and later) that lets any file or folder be stored in encrypted form and decrypted only by an individual user and an authorized recovery agent. EFS is especially useful for mobile computer users, whose computer (and files) are subject to physical theft, and for storing highly sensitive data.

FAT32 (File Allocation Table): The method that the operating systems use to keep track of files and to help the computer locate them on the disk. Even if a file is fragmented (split up into various areas on the disk), the file allocation table still can keep track of it. FAT32 is an improvement to the original FAT system, since it uses more bits to identify each cluster on the disk. This helps the computer locate files easier and allows for smaller clusters, which improves the efficiency of the hard disk. FAT32 supports up to two terabytes of hard disk storage.

Firewall: A method for implementing security policies designed to keep a network secure from intruders. It can be a single router that filters out unwanted packets or may comprise a combination of routers and servers each performing some type of firewall processing. Firewalls are widely used to give users secure access to the Internet as well as to separate an organization's public Web server from its internal network. Firewalls are also used to keep internal network segments secure; for example, the accounting network might be vulnerable to snooping from within the enterprise. In practice, many firewalls have default settings that provide little or no security unless specific policies are implemented by trained personnel. Firewalls installed to protect entire networks are typically implemented in hardware; however, software firewalls are also available to protect individual workstations from attack. While much effort has been made excluding unwanted input to the internal network, less attention has been paid to monitoring what goes out. Spyware is an application that keeps track of a user's Internet browsing habits and sends those statistics to a Web site.

The following are some of the techniques used in combination to provide firewall protection:

- 1) **Network Address Translation (NAT):** Allows one Internet Protocol (IP) address, which is shown to the outside world, to refer to many IP addresses internally, one on each client station. Performs the translation back and forth. NAT is found in routers and is built into Windows Internet Connection Sharing (ICS).
- 2) **Packet Filter:** Blocks traffic based on a specific Web address (IP address) or type of application (e-mail, File Transfer Protocol [FTP], Web, etc.), which is specified by port number. Packet filtering is typically done in a router, which is known as a screening router.
- 3) **Proxy Server:** Serves as a relay between two networks, breaking the connection between the two. Also typically caches Web pages.
- 4) **Stateful Inspection:** Tracks the transaction to ensure that inbound packets were requested by the user. Generally can examine multiple layers of the protocol stack, including the data, if required, so blocking can be made at any layer or depth.

IETF (Internet Engineering Task Force): The body that defines standard Internet operating protocols such as Transmission Control Protocol/Internet Protocol (TCP/IP). The IETF is supervised by the Internet Society Internet Architecture Board (IAB). IETF members are drawn from the Internet Society's individual and organization membership. Standards are expressed in the form of Requests for Comments (RFC).

Information security: The protection of data against unauthorized access. Programs and data can be secured by issuing identification numbers and passwords to authorized users. However, systems programmers or other technically competent individuals will ultimately have access to these codes. In addition, the password only validates that a correct number has been entered, not that it is the actual person. Using biometric techniques (fingerprints, eyes, voice, etc.) is a more secure method. Passwords can be checked by the operating system to prevent logging in. Database management system (DBMS) software prevents unauthorized access by assigning each user an individual view of the database. Data transmitted over networks can be secured by encryption to prevent eavesdropping. Although precautions can be taken to detect an unauthorized user, it is extremely difficult to determine if a valid user is purposefully doing something malicious. Someone may have valid access to an account for updating, but determining whether phony numbers are entered requires more processing. The bottom line is that effective security measures are always a balance between technology and personnel management.

IPSec (Internet Protocol Security): A security protocol from the IETF that provides authentication and encryption over the Internet. Unlike Secure Sockets Layer (SSL), which provides services at layer 4 and secures two applications, IPSec works at layer 3 and secures everything in the network. Also unlike SSL, which is typically built into the Web browser, IPSec requires a client installation. IPSec can access both Web and non-Web applications, whereas SSL requires a work around for non-Web access such as file sharing and backup. IPSec is supported by IPv6. Since IPSec was designed for the IP protocol, it has wide industry support and is expected to become the standard for virtual private networks (VPNs) on the Internet.

Kerberos: A security system developed at the Massachusetts Institute of Technology that authenticates users. It does not provide authorization to services or databases; it establishes identity at logon, which is used throughout the session.

Key: See Cryptographic key.

Keystroke logger: A program or hardware device that captures every key depression on the computer. Also known as keystroke cops, they are used to monitor an employee's activities by recording every keystroke the user makes, including typos, backspacing, and retyping.

LAN (Local Area Network): Any computer network technology that operates at high speed over short distances (up to a few thousand meters). A LAN may refer to a network in a given department or within a given firm or campus. It differs from computer networks that cross wider geographic spaces such as those networks on a wide area network (WAN). A LAN does not use the public arteries of the Internet like intranets and virtual private networks.

Management controls: Controls that include policies for operating information technology resources and for authorizing the capture, processing, storage, and transmission of various types of information. They also may include training of staff, oversight, and appropriate and vigorous response to infractions.

Need-to-know access: Under exceptional circumstances that are not stipulated in program policies, the case-by-case granting or denying of authorized access to case-specific information. This type of access is not routine; but rather it is for unusual situations and occurs only after careful deliberation by the ORP in concurrence with other public health professionals.

NIST (National Institute of Standards and Technology): Located in Washington, DC, it is the standards-defining agency of the U.S. government; formerly, the National Bureau of Standards. See <http://www.nist.gov>.

Nonpublic health uses of surveillance data: The release of data that are either directly or indirectly identifying to the public; to parties involved in civil, criminal, or administrative litigation; to nonpublic health agencies of the federal, state, or local government; or for commercial uses.

NTFS (NT File System): One of the file systems for the Windows NT operating system (and later). Windows NT also supports the FAT file system. NTFS has features to improve reliability, such as transaction logs to help recover from disk failures. To control access to files, you can set permissions for directories and/or individual files. NTFS files are not accessible from other operating systems such as DOS. For large applications, NTFS supports spanning volumes, which means files and directories can be spread out across several physical disks.

Overall Responsible Party (ORP): The official who accepts overall responsibility for implementing and enforcing these security standards and who may be liable for breach of confidentiality. The ORP should be a high-ranking public health official, for example, the division director or department chief over HIV/AIDS surveillance. This official should have the authority to make decisions about surveillance operations that may affect programs outside the HIV/AIDS surveillance unit and should serve as one of the contacts for public health professionals and the HIV-affected community on policies and practices associated with HIV/AIDS surveillance. The ORP is responsible for protecting HIV/AIDS surveillance data as they are collected, stored, analyzed, and released and must certify annually that all security program requirements are being met. The state's security policy must indicate the ORP by name.

Patch management: The installation of patches from a software vendor onto an organization's computers. Patching thousands of PCs and servers is a major issue. A patch should be applied to test machines first before deployment, and the testing environments must represent all the users' PCs with their unique mix of installed software.

Personal identifier: A datum, or collection of data, that allows the possessor to determine the identity of a single individual with a specified degree of certainty. A personal identifier may permit the identification of an individual within a given database. Bits of study data, when taken together, may be used to identify an individual. Therefore, when assembling or releasing databases, it is important to be clear which fields, either alone or in combination, could be used to such ends, and which controls provide an acceptable level of security.

Personnel controls: Staff member controls such as training, separation of duties, background checks of individuals, etc. Compare to physical and technical access controls.

PHIN MS (Public Health Information Network Messaging System): A generic, standards-based, interoperable, and extensible message transport system. It is platform-independent and loosely coupled with systems that produce outgoing messages or consume incoming messages.

Physical access controls: Controls involving barriers, such as locked doors, sealed windows, password-protected keyboards, entry logs, guards, etc. Compare to personnel and technical access controls.

PKI (Public Key Infrastructure): A secure method for exchanging information within an organization, an industry, a nation, or worldwide. A PKI uses the asymmetric encryption method (also known as the public/private key method) for encrypting IDs and documents/messages. Also, see Cryptography. It starts with the certificate authority (CA), which issues digital certificates (digital IDs) that authenticate the identity of people and organizations over a public system such as the Internet. The PKI can also be implemented by an enterprise for internal use to authenticate users that handle sensitive information. In this case, the enterprise is its own CA. The PKI also establishes the encryption algorithms, levels of security, and distribution policy to users. It not only deals with signed certificates for identity authentication, but also with signed messages, which ensures the integrity of the message so the recipient knows it has not been tampered with. The PKI also embraces all the software (browsers, e-mail programs, etc.) that supports the process by examining and validating the certificates and signed messages.

Plaintext: Normal text that has not been encrypted and is readable by text editors and word processors. Contrast with ciphertext.

Private key: The private part of a two part, public key cryptography system. The private key is kept secret and never transmitted over a network.

Project areas: HIV/AIDS surveillance sites that are directly funded by CDC. The HIV/AIDS surveillance project areas are the 50 states, the District of Columbia, San Francisco, Los Angeles, Chicago, Houston, New York City, Philadelphia, Puerto Rico, U.S. Virgin Islands, Guam, American Samoa, the Republic of the Marshall Islands, the Commonwealth of the Northern Mariana Islands, the Republic of Palau, and the Federated States of Micronesia.

Provider: Any source of HIV/AIDS surveillance information, such as a physician, nurse, dentist, pharmacist, or other professional provider of health care or a hospital, health maintenance organization, pharmacy, laboratory, STD clinic, TB clinic, or other health care facility that forwards data into the surveillance system.

Public health uses of surveillance data: The principal public health use of HIV/AIDS surveillance at state and federal levels is for epidemiologic monitoring of trends in disease incidence and outcomes. This includes collection of data and evaluation of the collection system, as well as the reporting of aggregate trends in incidence and prevalence by demographic, geographic, and behavioral risk characteristics to assist the formulation of public health policy and direct intervention programs.

Surveillance data may be used for public health and epidemiologic research. Data that include names may be collected and released to public health officials on individual cases or clusters of cases of HIV/AIDS that are of particular epidemiologic or public health significance, such as those associated with new or unusual modes of HIV transmission, the detection of unusual strains of HIV, or the occurrence of unusual laboratory or clinical profiles. Analysis of these data may result in the formulation of public health recommendations for standards of diagnosis and treatment of HIV/AIDS and for preventing HIV transmission. However, when such data are released or reported to persons not having role-based or need-to-know access, information shall be presented in such a way as to preclude direct or indirect identification of individuals (e.g., by obscuring geographic or institutional affiliations).

The use of surveillance data to prompt follow-up by health departments with individual patients or their health care providers may constitute legitimate public health practice. In the context that the health department functions as the primary provider of care for persons who seek HIV counseling and testing, diagnosis and treatment of STDs, or medical and social services, health department staff may interact directly with their clients, independently of the role of the health department in monitoring epidemiologic trends in the incidence of HIV/AIDS. Where states or local communities determine that health departments should offer referrals to services for persons whose names are reported to the HIV/AIDS surveillance system and who are not primarily health department clients, and where the surveillance data serve as the source of identification of such individuals, health departments should establish standards and principles for such practice in collaboration with providers and community partners. This helps ensure the security and confidentiality protections are in place.

Public key: The published part of a two part, public key cryptography system. The private part is known only to the owner.

Quality improvement: Activities to enhance the performance level of a process. Quality improvement efforts involve measurement of the current level of performance, development of methods to raise that level, and implementation of those methods.

RAM (Random-Access Memory): A type of computer memory that can be accessed randomly; that is, any byte of memory can be accessed without touching the preceding bytes. RAM is the most common type of memory found in computers and other devices, such as printers. There are two basic types of RAM, dynamic RAM (DRAM) and static RAM (SRAM).

The two types differ in the technology they use to hold data, dynamic RAM being the more common type. Dynamic RAM needs to be refreshed thousands of times per second. Static RAM does not need to be refreshed, which makes it faster; but it is also more expensive than dynamic RAM. Both types of RAM are volatile, meaning that they lose their contents when the power is turned off.

Records retention policy: Assigning a length of time and date to paper or electronic records to establish when they should be archived or destroyed.

Risk: In the context of system security, the likelihood that a specific threat will exploit certain vulnerabilities and the resulting effect of that event. A thorough and accurate risk analysis would consider all relevant losses that might be expected if security measures were not in place. Relevant losses can include losses caused by unauthorized uses and disclosures and loss of data integrity that would be expected to occur absent the security measures. One of the reasonable risks that are identifiable is that someone could inadvertently or purposely make an unauthorized change to data that could affect patient care. Another reasonable integrity risk is that data may be lost or modified in transmission. Software bugs, viruses and worms, hardware malfunctions, and natural disasters such as fire or flood also can compromise data integrity.

Risk management: The optimal allocation of resources to arrive at a cost-effective investment in defensive measures for minimizing both risk and costs in a particular organization.

Role-based access: Access to specific information or data granted or denied by the ORP depending on the user's job status or authority. Roles typically group users by their work function. This control mechanism protects data and system integrity by preventing access to unauthorized applications. In addition, defining access based on roles within an organization, rather than by individual users, simplifies an organization's security policy and procedures. Compare to need-to-know access.

ROM (Read-Only Memory): Computer memory on which data have been prerecorded. Once data have been written onto a ROM chip, they cannot be removed and can only be read. Unlike main memory (RAM), ROM retains its contents even when the computer is turned off. ROM is referred to as being nonvolatile, whereas RAM is volatile.

Most personal computers contain a small amount of ROM that stores critical programs such as the program that boots the computer. In addition, ROM is used extensively in calculators and peripheral devices such as laser printers, whose fonts are often stored in ROM. A variation of a ROM is a PROM (programmable read-only memory). PROMs are manufactured as blank chips on which data can be written with a special device called a PROM programmer.

RSA (Rivest-Shamir-Adleman): A highly secure cryptography method by RSA Security, Inc., Bedford, MA (www.rsa.com). It uses a two part key. The private key is kept by the owner; the public key is published.

Data are encrypted by using the recipient's public key, which can only be decrypted by the recipient's private key. RSA is very computation intensive; thus it is often used to create a digital envelope, which holds an RSA-encrypted DES key and DES-encrypted data. This method encrypts the secret DES key so that it can be transmitted over the network, but encrypts and decrypts the actual message using the much faster DES algorithm.

RSA is also used for authentication by creating a digital signature. In this case, the sender's private key is used for encryption, and the sender's public key is used for decryption. See Digital signature.

The RSA algorithm is also implemented in hardware. As RSA chips get faster, RSA encoding and decoding add less overhead to the operation.

Sanitize: Also known as disk wiping, sanitizing is the act of destroying the deleted information on a hard disk or floppy disk to ensure that all traces of the deleted files are unrecoverable. Software programs that can successfully sanitize a diskette are available.

Script kiddie: A person who uses scripts and programs developed by others for the purpose of compromising computer accounts and files, and launching attacks on whole computer systems; in general, these persons do not have the ability to write said programs on their own. Normally, this person is someone who is not technologically sophisticated and who randomly seeks out a specific weakness over the Internet to gain root access to a system without really understanding what is being exploited because the weakness was discovered by someone else. A script kiddie is not looking to target specific information or a specific organization, but rather uses knowledge of a vulnerability to scan the entire Internet for a victim that possesses that vulnerability.

Secret key cryptography: Using the same secret key to encrypt and decrypt messages. The problem with this method is transmitting the secret key to a legitimate person who needs it.

Secured area: The physical confinement limiting where confidential HIV/AIDS surveillance data are available. Only authorized staff have access to this area. The secured area usually is defined by hard, floor-to-ceiling walls with a locking door and may include other measures (e.g., alarms, security personnel).

Security: The protection of surveillance data and information systems, with the purposes of

- 1) preventing unauthorized release of identifying surveillance information or data from the systems (e.g., preventing a breach of confidentiality) and
- 2) protecting the integrity of the data by preventing accidental data loss or damage to the systems.

Security includes measures to detect, document, and counter threats to the confidentiality or integrity of the systems.

Server farm: A group of network servers that are housed in one location. A server farm provides bulk computing for specific applications such as Web site hosting; in contrast, although a data center has many servers, it also has people. In a server farm, a user would generally only see a technician when an installation or a repair was performed; whereas in the data center, operators would be sitting at consoles, putting paper in printers, and possibly moving disks and tapes from one place to another. A server farm is typically a room with dozens, hundreds, or even thousands of rack-mounted servers humming away. They might all run the same operating system and applications and use load balancing to distribute the workload between them.

Smart cards: A credit card sized card with a built-in microprocessor and memory used for identification or financial transactions. When inserted into a reader, it transfers data to and from a central computer. It is more secure than a magnetic stripe card and can be programmed to self-destruct if the wrong password is entered too many times. As a financial transaction card, it can be loaded with digital money and used like a travelers check, except that variable amounts of money can be spent until the balance is zero.

Spyware: Software that sends information about Web surfing habits to its Web site. Often quickly installed on a computer in combination with a free download purposefully selected from the Web, spyware (also known as parasite software or scumware) transmits information in the background as a user moves around the Web.

The license agreement may or may not clearly indicate what the software does. It may state that the program performs anonymous profiling, which means that a user's browsing habits are being recorded. Such software is used to create marketing profiles. For example, a person who accesses Web site A, often accesses Web site B and so on. Spyware can be clever enough to deliver competing products in real time. For example, if a user accesses a Web page to look for a minivan, an advertisement for a competitor's minivan might pop up.

Spyware organizations argue that as long as they are not recording names and personal data, but treat the user as a numbered individual who has certain preferences, they are not violating a person's right to privacy. Nevertheless, many feel their privacy has been violated. The bottom line is that once users detect a spyware program in their computer, it can be eliminated, albeit sometimes with much difficulty. The downside is that people can become suspect of every piece of software they install.

SSL (Secure Sockets Layer): The leading security protocol on the Internet. When an SSL session is started, the server sends its public key to the browser, which the browser uses to send a randomly generated secret key back to the server in order to have a secret key exchange for that session. Developed by Netscape, SSL has been merged with other protocols and authentication methods by the IETF into a new protocol known as Transport Layer Security (TLS).

Super user: Someone with the highest level of user privilege who can allow unlimited access to a system's file and setup. Usually, super user is the highest level of privilege for applications, as opposed to operating or network systems. A super user could destroy the organization's systems maliciously or simply by accident.

Surveillance: The ongoing and systematic collection (paper or electronically), analysis, and interpretation of health data in the process of describing and monitoring a health event. This information is used for planning, implementing, and evaluating public health interventions.

Surveillance data: Statistics generated from disease surveillance in either paper or electronic format.

Surveillance information: Details collected on an individual or individuals for completing routine or special surveillance investigations. Examples of HIV/AIDS surveillance information are the HIV/AIDS report forms, ancillary notes about risk investigations and related questionnaires, notes about suspect cases, laboratory reports, ICD9/10 line lists, discharge summaries, death certificates, and drug data stores.

Symmetric encryption: Same as secret key cryptography.

Technical access controls: Controls involving technology, such as requirements for password use and change, audit of the electronic environment, access to data controlled through known software tools, and control over introduction of changes to the information technology environment (hardware, software, utilities, etc.). Compare to personnel and physical access controls.

Trojan horse: A program that appears legitimate, but performs some illicit activity when it is run. It may be used to locate password information, make the system more vulnerable to future entry, or simply destroy programs or data on the hard disk. A Trojan horse is similar to a virus, except that it does not replicate itself. It stays in the computer doing its damage or allowing somebody from a remote site to take control of the computer. Trojans often sneak in attached to a free game or other utility.

Two-factor authentication: The use of two independent mechanisms for authentication; for example, requiring a smart card and a password. The combination is less likely to allow abuse than either component alone.

Virus: Software program first written by Fred Cohen in 1983, and later coined in a 1984 research paper. A virus is a software program, script, or macro that has been designed to infect, destroy, modify, or cause other problems with a computer or software program. Installing an antivirus protection program can help prevent viruses.

VPN (Virtual Private Networks): A network that is connected to the Internet, but uses encryption to scramble all the data sent through the Internet so the entire network is "virtually" private.

Vulnerability: A security exposure in an operating system or other system software or application software component. Security firms maintain databases of vulnerabilities based on version number of the software. Any vulnerability can potentially compromise the system or network if exploited. For a database of common vulnerabilities and exposures, visit <http://icat.nist.gov/icat.cfm>.

WAN (Wide Area Network): A network of computers that can span hundreds or thousands of miles. Unlike intranets and virtual private networks, a WAN does not use public Internet arteries and is isolated from the public domain.

Zombie: A computer system that has been covertly taken over to transmit phony messages that slow down service and disrupt the network. A pulsing zombie sends bogus messages in periodic bursts rather than continuously.

Attachment G

Using HIV Surveillance Data to Document Need and Initiate Referrals

Introduction to the Issue5-2

Contents

Background Information for the Surveillance Coordinator5-4

- How should HIV/AIDS surveillance data be used?
- What types of patient services might patients be referred to through the use of individual case reports?
- What are partner counseling and referral services (PCRS) and how are they carried out?
- What is HIV prevention case management?
- How do some health departments use individual HIV case reports to initiate referrals for prevention and medical services?
- What are CDC's recommendations regarding the use of HIV surveillance data for referrals to patient services, such as prevention case management or PCRS?
- What issues should health departments and communities consider before making the decision to use confidential information obtained through HIV/AIDS surveillance for PCRS or case management services?
- What steps should local areas take when developing appropriate procedures for using surveillance data to initiate referrals to patient services?
- Are health department staff required to contact those who are reported through HIV surveillance?

Handouts5-10

- Using HIV Surveillance Data: Focus on New Jersey
- Frequently Asked Questions about HIV Surveillance and its Relationship to Prevention and Treatment Services

Introduction to the Issue

The primary objective of population-based HIV case surveillance is to allow state and local health departments to monitor changing trends in the HIV epidemic and thereby direct available resources to where they are needed most. For this purpose, CDC strongly recommends the use of summary statistics with identifying information removed. This Toolkit provides information and resources to help HIV/AIDS surveillance coordinators develop principles for the use of the HIV/AIDS surveillance database to document need and evaluate services.

Although the HIV surveillance system was not designed for case management purposes, some states and territories have chosen to use individual case reports to offer HIV-infected individuals referrals to voluntary prevention and care services. States that are using the HIV surveillance database for this purpose should follow established guidelines and standards for maintaining security and confidentiality of HIV surveillance information. States implementing HIV case surveillance and considering using case reports as a basis for offering voluntary referrals to prevention and treatment programs should do so only when principles and practices are developed locally in collaboration with community partners. The collaborative process should include developing explicit protocols with appropriate clearances that establish practices for contacting providers and patients and ensure that security and confidentiality protections are in place if information from HIV/AIDS surveillance is used to initiate any contact with patients.

Finally, both CDC and CSTE have stated that partner counseling and referral services (PCRS), formerly known as partner notification, activities do not necessarily have to be linked to HIV reporting in order to be effective public health tools. All states currently conduct partner notification activities regardless of whether they have HIV surveillance. Furthermore, some states have initiated HIV surveillance exclusive of PCRS programs. Therefore, CDC and CSTE suggest support for voluntary PCRS should be developed in the broader context of HIV prevention community planning or other advisory processes and should not be necessarily coupled with HIV surveillance. If established, linkages of surveillance and prevention services should neither compromise the quality and security of the surveillance system nor compromise the quality, confidentiality, and voluntary nature of prevention services.

This Toolkit can help guide discussions between surveillance staff and prevention programs and community advisory groups on the ways in which information from the HIV/AIDS surveillance database may be used as a mechanism for referring HIV-infected individuals to prevention, medical, and social services when areas decide to do so locally. The various HIV-related services that patients and their providers may choose are described. In addition, the Toolkit outlines some issues that should be considered before making the decision to use HIV surveillance in this way, suggests alternative strategies, and outlines a process for deliberations.

This Toolkit:

- reviews in question and answer format some issues surveillance staff and stakeholders must consider when discussing how HIV/AIDS surveillance data may be used to provide referrals for HIV-related prevention and medical services, and
- provides materials that may be useful in discussions with stakeholders.

The *Resource Manual's Appendix*, bound separately, contains the following background resources that provide more comprehensive information on the issues and on current CDC guidelines and practices:

- CDC. Public health uses of HIV-infection reports—South Carolina, 1986-1991. *Morbidity and Mortality Weekly Report* 1992;41(15):245-249. (Located in the Toolkit 1 section of the Appendix.)
- CDC. U.S. Public Health Service Recommendations for human immunodeficiency virus counseling and voluntary testing for pregnant women. July 7, 1995. *Morbidity and Mortality Weekly Report* 44 (No. RR-7).
- CSTE. National HIV Surveillance: Addition to the National Public Health Surveillance System. 1997 CSTE Annual Meeting Position Statement #ID-4. (Located in the Toolkit 1 section of the Appendix.)
- Fenton KA, Peterman TA. HIV partner notification: taking a new look. *AIDS* 1997;11(13):1535-1546.
- West GR, Stark KA. Partner notification of HIV prevention: a critical reexamination. *AIDS Education and Prevention* 1997;9(Supplement B):68-78.

In addition, surveillance coordinators may want to consult these two resources, which CDC has distributed separately:

- CDC. *Draft HIV Partner Counseling and Referral Services Operational Guidelines*. October, 1998.
- CDC. *HIV Prevention Case Management—Guidance*. September 1997.

Background Information for the Surveillance Coordinator

As surveillance officers and their staffs work with prevention programs and community representatives, they may receive questions about how individual surveillance data may be used by health departments for purposes of referral to services or other program activities. This section provides background information, organized by questions that may be raised, to help surveillance staff explain CDC recommendations, discuss the implications and answer questions about the issues.

- ☞ This symbol points out further supporting materials contained in Toolkit 5 or directs the reader to related materials in other Toolkits.

How should HIV/AIDS surveillance data be used?

HIV and AIDS data should be used to monitor changing epidemiologic trends in incidence and outcomes, assist in formulating public health policy, document the need for services, and direct available resources for targeted prevention interventions for persons with HIV. This is done through the use of aggregate data. Aggregate data include summary statistics compiled from personal information, but grouped to preclude identification of individual cases. For example, the number and characteristics of persons living with HIV by geographic area may be used to determine the distribution of local care services or assess the need for drug assistance programs. HIV data may also be used to set priorities among areas and groups at risk that might benefit from targeted HIV testing and counseling programs.

Together with local community advisory groups, health departments may determine that another appropriate use of surveillance data is to use individual-level data from HIV surveillance registries to prompt follow up by the health department with patients or providers to offer voluntary referrals for various patient services. Individual-level data include case specific data where individuals are identified. There is no CDC requirement that surveillance programs share individual case reports with prevention or care programs. To be consistent with the federal assurance of confidentiality under which CDC collects HIV/AIDS surveillance data and the purpose for which CDC provides support to states to conduct HIV/AIDS surveillance, individual-level surveillance data should not be used to directly or indirectly identify an individual for non-public health purposes, such as the release of individual-level data to the public, to parties involved in civil, criminal, or administrative litigation, or to non-health agencies of the federal, state, or local government.

- ☞ *Using HIV Surveillance Data: Focus on New Jersey* is a handout that summarizes that state's experiences using aggregate HIV surveillance data for planning and policy purposes.

What types of patient services might patients be referred to through the use of individual case reports?

This might include a wide range of care services, such as medical treatment, social or support services, or laboratory testing, including CD4+T-lymphocyte testing. In addition, prevention services, such as assistance with notifying sex and needle-sharing partners, prevention case management, and counseling and testing services, may also be offered.

What are partner counseling and referral services (PCRS) and how are they carried out?

The goals of PCRS are to provide services to sex and needle-sharing partners of HIV-infected individuals and to help partners gain access to individualized counseling, testing, medical evaluation, treatment, and other prevention services. It is a means of alerting individuals who may not know they have been exposed to HIV through sexual contact or needle-sharing practices to the possible need for testing and medical services. It also is a means of reaching individuals early in the disease process so they are able to more quickly take advantage of new therapies for treatment of HIV infection and opportunistic infections. Prevention education and risk reduction services are also important for those exposed to HIV to help prevent further spread in the community.

Partners may be notified either by the individual who has been diagnosed with HIV, by his or her health care provider, or by a health professional from the health department. HIV infected persons do not have to reveal their partners to their physicians or to the health department to receive needed medical services. In many cases, the individual is coached on ways to notify his or her own partners and provided with information that partners will need to seek testing and other services.

If partners are contacted by health department staff, they are referred to testing and other support services, and their confidentiality is under the same laws, rules, and mechanisms that apply to HIV-infected individuals. Partners' decisions to seek services are entirely voluntary. For more detailed information on PCRS, surveillance coordinators can contact the CDC Community Assistance, Planning, and National Partnerships Branch (CAPNP) HIV prevention project officer, who can provide copies of the *Draft HIV Partner Counseling and Referral Service Operational Guidelines*—October 7 1998.

What is HIV prevention case management?

HIV Prevention Case Management (PCM) is a client-centered HIV prevention activity with the goal of promoting the adoption and maintenance of HIV risk-reduction behaviors by clients with multiple complex problems and risk-reduction needs. It is a hybrid of HIV risk reduction counseling and traditional case management that includes intensive, ongoing, individualized prevention counseling, support, and service brokerage. CDC provides funding and technical assistance for individual-level health education and risk-reduction activities, including PCM. Guidance for planning, implementing, and evaluating PCM is provided in *HIV Prevention Case Management-Guidance. September 1997.*, which may be obtained through the CDC National AIDS Clearinghouse at 1-800-458-5231.

How do some health departments use individual HIV case reports to initiate referrals for prevention and medical services?

Some states have instituted local policies that allow individual case reports to be used to trigger follow-up activities by the health department in which individuals are referred to prevention and treatment services. Areas with these linkages primarily do so to facilitate offering services to persons tested in non-public health clinic settings, because follow up with health department clients (i.e., persons tested in public STD clinics or counseling and testing sites) to provide referrals to appropriate prevention and care services is routine. Contacting non-health department reporting sources (e.g., hospitals, private physicians, clinics, or blood banks) may be done to provide training and education regarding conduct of PCRS, provide information about available services, or seek permission to contact patients.

Because the majority of persons reported with HIV infection are tested in medical settings (not public health clinics), areas considering offering referrals for services (e.g., PCRS) based on surveillance case reports should carefully consider if there is a need to follow up with patients tested and reported by private providers (e.g., private physicians, HMOs). Offering assistance with post-test counseling or referrals to test providers that do not routinely provide medical or prevention services (e.g., blood banks or laboratories) may also be considered. Policies regarding contact by health department staff of persons tested in non-health department settings should be developed locally by health departments in collaboration with communities and providers. For health department staff to directly contact patients tested by a non-health department provider without first contacting that provider may be seen as intrusive and be an inefficient use of public health resources. Follow up by health department staff of persons reported with HIV should be conducted with the participation of the physician or provider who ordered the HIV antibody test. In some states, the health department must always obtain permission from the HIV-infected individual's physician before contacting that person. Although surveillance staff may inquire about the patient's need for services and referrals while following up on case reports or when obtaining complete data (e.g., risk information) from a provider, surveillance staff should not be responsible for contacting patients to provide these referrals. Rather, health department staff who are responsible for PCRS or patient case management should initiate the contact following locally established procedures. The figure on page 5-9 diagrams an example of how this contact should take place.

Some examples of locally developed procedures for using individual case reports to initiate patient services include:

In Minnesota, all persons testing HIV positive are contacted by health department staff and provided, on a voluntary basis, with referrals for case management, assistance with obtaining Medicaid and drug assistance, and partner notification services. After receiving HIV positive reports from laboratories and other sources, surveillance provides information to designated prevention staff who then coordinate contact with patients. Information from surveillance is provided on a case-by-case basis to prevention staff at weekly sessions using a confidential process. HIV prevention staff try to work with providers to ensure that the doctor or doctor's staff has a chance to discuss health

department support services with the patient first. This gives the patient some advance notice to expect a contact from the health department and an opportunity to ask questions of a familiar provider. This discussion may relieve some of the anxiety or fear that individuals may experience when health department contact is unexpected or not understood. HIV surveillance and prevention staff believe this increases patient and provider cooperation with health department programs.

- In Missouri, the health department seeks permission from providers before contacting patients tested in the private sector. Surveillance staff obtain physician approval to contact a patient tested in and reported from the private sector while they are obtaining information that was not included with the original case report. If the provider thinks follow up with the patient is appropriate, surveillance staff share the individual case report with designated health department staff, who distribute cases for follow up to local field investigators. Disease investigators offer PCRS and inform the patient about the availability of "service coordination" in their state.
- ☞ *Frequently Asked Questions about HIV Surveillance and its Relationship to Prevention and Treatment Services* is a handout that describes surveillance's links to services and partner notification.

What are CDC's recommendations regarding the use of HIV surveillance data for referrals to patient services, such as prevention case management or PCRS?

CDC maintains that individual HIV case data need not be used directly to initiate prevention or patient services. Rather, aggregate surveillance data can be used to direct non-surveillance health department staff (e.g., case managers, disease investigators) to providers or reporting sources to advise them of available prevention and services for their patients. If providers ask for assistance, areas should follow locally-established protocols and procedures to respond to provider and patient needs.

Ultimately, CDC considers the decision to use HIV surveillance to initiate case management services or referrals to other services to be a local decision. If established, these linkages should not compromise the quality or security of the surveillance system nor compromise the quality, confidentiality, and voluntary nature of prevention case management or other services. Methods undertaken should not jeopardize support for representative, complete, and timely case reporting or be inconsistent with CDC required standards for security and confidentiality of HIV/AIDS surveillance data. If areas, with the concurrence of community planning groups, elect to share individual case data from surveillance with other programs, the recipients of the surveillance information should be subject to the same penalties for unauthorized disclosure as are surveillance personnel. In addition, prevention programs that use HIV surveillance case data should evaluate the effectiveness of this approach and the program's policies and practices that protect against breaches of confidentiality.

- See *Security Standards for Protection of HIV/AIDS Surveillance Information and Data. Appendix C: Guidelines for HIV/AIDS Surveillance—1998* for information regarding security and confidentiality standards for HIV data.

What issues should health departments and communities consider before making the decision to use confidential information obtained through HIV/AIDS surveillance for PCRS or case management services?

There are two key issues that health departments should consider before deciding to use data for PCRS or case management:

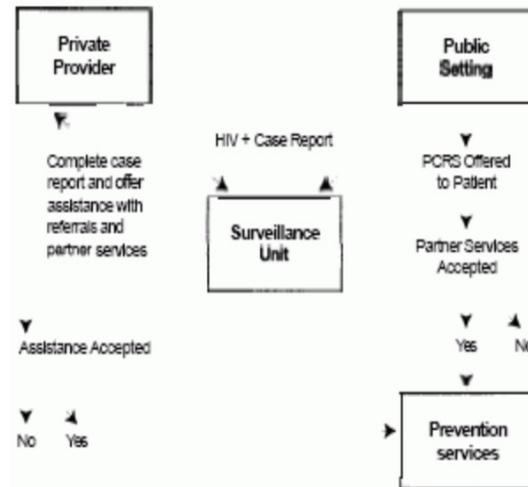
Whether linking surveillance for referrals to patient services may affect the acceptability of the system. Linking HIV surveillance to services may adversely affect the acceptability of HIV surveillance by the community and providers because it may be perceived as an unauthorized release of information from the surveillance system. One way of increasing acceptability may be to involve physicians in the process. For example, if case reports result in referrals from surveillance to other health department staff for the purpose of offering prevention services, health care providers should be contacted before notifying the patient and offered an opportunity to say whether follow up with the individual is appropriate or necessary. Physicians should be encouraged to counsel their patients about the probability of a health department visit (as local policy dictates) so the patient can be prepared for or expect the initial contact and understand its purpose. In one state, the patient is given the option of calling appropriate health department staff himself or herself and is therefore put in control of the process. This option enables the patient to preserve his or her confidentiality.

Whether there are alternative strategies for offering PCRS or case management that might be more feasible, timely, and efficient and that do not require the use of individual HIV/AIDS case reports. HIV surveillance and PCRS activities do not need to be linked in order to be effective public health tools. For example, focusing PCRS activities or referrals to other services in places where clients are present at public clinics and counseling and testing sites may be more efficient programmatically, less intrusive to individuals, ensure more timely provision of such services, and does not require a direct link to surveillance case reports. Public health providers can then ensure discussion of the PCRS process during pretest counseling in a controlled and confidential environment. Focused PCRS activities may facilitate client-centered counseling methods and allow for better referrals to treatment and other care services. Another strategy that does not require linkage to surveillance might include providing targeted testing services in high prevalence areas. Areas may also choose to target education to large providers of HIV care and assist in developing mechanisms of referral for health department services when needed. In some states, health department staff train physicians to provide partner services and referrals and only contact the provider's patients at the provider's request.

What steps should local areas take when developing appropriate procedures for using surveillance data to initiate referrals to patient services?

If a health department and community together decide to use surveillance data to initiate PCRS or case management, they should discuss the flow of information in detail, develop a protocol, and conduct a pilot of the proposed system. (The figure shows an example of information flow in public and private settings.) The protocol should include objectives and cover practical considerations such as what information will be released, who will have access to it, what security measures will be in place (particularly if information is shared outside of surveillance), and how the system will be evaluated. Data should not be shared with programs that do not have well defined public health objectives or with programs that cannot guarantee confidentiality. Prevention programs that receive surveillance information must be subject to the same penalties for unauthorized disclosure as are surveillance programs, and they must maintain the shared data in a secure and confidential manner. At a minimum, areas should develop a written protocol, and pilot test the system in one or two areas before widespread implementation to ensure procedures are appropriate, and that the system achieves stated goals and objectives and is acceptable to providers and the community.

Example of Information Flow for Case Reports and Service Referrals from Public and Private Settings



Are health department staff required to contact those who are reported through HIV surveillance?

There is no federal requirement that health department staff contact HIV-infected individuals or their sex or needle-sharing partners. However, as a condition of HIV prevention funding, CDC requires all state HIV prevention programs to "establish standards, implement, and maintain procedures for confidential, voluntary, client-centered counseling and referral of sex and needle-sharing partners of HIV infected persons, consistent with the current CDC Partner Counseling and Referral Services Guidance" and "maintain their good faith effort to notify spouses of infected persons as required by law and as certified to CDC" regardless of the state's HIV reporting laws. CDC and CSTE have stated that HIV surveillance and PCRS activities do not need to be linked in order to be effective public health tools.

Using HIV Surveillance Data: Focus on New Jersey

New Jersey was the first state with high HIV prevalence to include HIV reporting in its surveillance system. New Jersey added HIV surveillance to its existing AIDS surveillance system in October 1991 and began reporting case data in January 1992. Since that time, the state has used aggregate HIV surveillance data to improve its ability to monitor the epidemic. In turn, this enhanced monitoring capability has allowed public health workers to better target prevention and treatment services for HIV-infected people, and also has served as a basis for policy decisions and program evaluation.

Improved Prevention Planning and Priority Setting

Surveillance data are used to inform the community prevention planning process. Community planning groups, made up of local representatives from public health and community organizations serving persons with HIV and members of the infected community, currently dictate the targeted populations and geographic distribution of funded activities for street and community outreach, health education risk reduction sessions, and prevention case management. Surveillance data help planners set priorities and reassess need for services in their communities.

Bridgeton, New Jersey is a classic example of the use of HIV data in prevention planning. According to AIDS reports from Bridgeton through 1997, women accounted for 24% of the patients, men accounted for 76% of the patients and the 20- to 29-year-old age range accounted for only 9% of the patients.

However, as shown here, HIV data showed a completely different picture. According to HIV reports from Bridgeton, women accounted for 43% of the cases, men accounted for 57% of the cases, and the 20- to 29-year-old age range accounted for 39% of the patients, making it the age range with the largest number of cases. The HIV data provided a more accurate picture of where the epidemic existed and where it was headed. In contrast, AIDS information showed only where the epidemic had been.

Brighton, NJ: Data through 12/31/97

	AIDS Data	HIV Data
Women	24%	43%
Men	76%	57%
20-29 Year Olds	9%	39%

Based on the information provided by HIV surveillance data, Bridgeton initiated a targeted prevention program for younger women and youth. It includes multiple ongoing small group sessions and prevention case management for women and youth.

Resource Management and Funding Allocation

Drug Assistance. Many states have been concerned that adding new antiretroviral therapies to their AIDS drug distribution program would drain resources and necessitate limiting enrollment into the program. When the question of adding these new medications to New Jersey's drug assistance program arose, the state was able to base its decision, in part, on an economic model formulated from the estimated number of people in New Jersey living with HIV or AIDS. HIV surveillance provided critical data on the potential number of infected persons and the percentage that would be eligible for the program. While many states have had to modify their eligibility criteria, New Jersey was able to add all of the new antiretroviral agents and remain solvent without modifying the eligibility criteria.

Better Directing of Treatment Resources. The number of people living with HIV and AIDS is used for planning purposes because it provides a more accurate representation of the number of people who will require care in a specific geographic area. New Jersey and other states are working toward a more equitable overall funding of Ryan White money per case.

Evaluation of Perinatal Prevention Efforts

Evaluating Public Health Recommendations.

HIV data have played an important role in evaluating the implementation of the public health service recommendations for the prevention of mother-to-infant (perinatal) HIV transmission in New Jersey. Because New Jersey has name-based HIV reporting, public health officials have been able to follow children who were exposed to HIV perinatally to determine their final HIV status. Aggregate HIV surveillance data have been used to monitor Zidovudine (ZDV) use in pregnant women and subsequent trends in perinatal transmission. The percentage of children infected as a result of perinatal HIV exposure in New Jersey decreased from 22% in 1993 to 15% in 1995. HIV data also indicated that the HIV status of 96% of HIV positive pregnant women was known at or before birth.

Argue Against Mandatory Testing. HIV data have been used to inform the Medical Society of New Jersey and the New Jersey legislature, the Governors AIDS Advisory Council, and the National Academy of Sciences/Institute of Medicine Committee on Perinatal HIV Transmission, that the New Jersey law requiring mandatory HIV counseling and voluntary testing for all pregnant women appears to be working well in New Jersey, and there is no need for mandatory testing of newborns.

Tracking Emerging Issues of Public Health Importance

Monitoring Recent Infection. HIV surveillance data are used to characterize persons likely to have recently acquired their HIV infection based on documented recent seroconversion, persons with high CD4 counts, and young persons recently diagnosed with HIV. Aggregate HIV surveillance data in New Jersey are used to help identify where new infections may be occurring and describe risk exposure associated with recent infection. HIV data on persons with recent HIV infection in New Jersey is being used to guide more focused research on circumstances surrounding testing, previous sexual and drug-using behaviors that may have been associated with HIV transmission, as well as current behaviors among persons with recent HIV infection.

Keeping a Watch for Unusual HIV Strains. HIV, a pathogen that mutates extensively, presents significant challenges to effective disease control. In the United States, the most common HIV strain is identified as HIV-1, Group M, Subtype B. Data from New Jersey's HIV surveillance system formed the basis of special studies to detect variant strains of HIV in the state. The first U.S. case of HIV-2, a type primarily found in West Africa, was identified in New Jersey through the surveillance system. An additional study led to the identification of variant strains of HIV in the state. Information from HIV surveillance provided public health officials with the basic information to guide development of a separate system to detect variant strains of HIV, and this is now in place in New Jersey. Understanding variations of HIV will help ensure that diagnostic tests will be able to detect the virus both for proper testing and to protect the safety of the blood supply.

Frequently Asked Questions on HIV Surveillance and its Relationship to Prevention and Treatment Services

How should HIV/AIDS surveillance data be used to direct services?

In addition to monitoring changing epidemiologic trends, HIV and AIDS data should be used to assist in formulating public health policy, documenting the need for services, and directing available resources for targeted prevention interventions for persons with HIV. This is done through the use of summary HIV data. For example, the number and characteristics of persons living with HIV by geographic area may be used to determine the distribution of local care services or assess the need for drug assistance programs. HIV data may also be used by communities and health officials to set priorities among areas and groups at risk that might benefit from targeted HIV testing and counseling programs, redistribution of drug assistance programs, or community outreach and education programs.

When people with HIV are reported to the health department, do they automatically get prevention and treatment services?

No. There is no automatic or recommended link between HIV surveillance and prevention services. All states have programs in place to offer voluntary partner counseling and referral services (PCRS) regardless of whether the state requires HIV reporting or not. In addition, some states also offer referrals for treatment services to patients seen within the public health clinic system.

Some states use HIV case data to trigger referrals of individuals to services. However, the extent to which individual HIV case data are used to facilitate access to prevention and care services varies from state to state, depending on factors such as resources, the available array of services, and community concerns about release of confidential information for purposes other than surveillance.

What is the linkage between HIV surveillance programs and HIV prevention case management and care programs?

CDC considers that the decision to link surveillance with case management services should be made at the local level and should be developed in the broader context of HIV prevention community planning or other advisory processes. If established, these linkages should not compromise the quality or security of the surveillance system nor compromise the quality, confidentiality, and voluntary nature of prevention case management services. Although CDC is not directly responsible for the delivery of medical care for persons with HIV, CDC does provide funds for state and local programs to facilitate the referral from HIV counseling and testing programs and health education risk reduction programs to HIV care facilities.

How do some health departments use HIV case reports to assist in offering referrals to services?

Prevention services and referrals are routinely offered to persons testing HIV positive in health department clinics and counseling and testing sites. However, the extent to which health departments use HIV data to assist in offering services to persons tested in other settings varies. When persons are reported with HIV from non-health department providers, such as physicians and HMOs, health departments offer services through or with the participation of the physician or provider who ordered the HIV antibody test. For example, health department staff may contact the provider to offer information on services available to their patient or they may discuss meeting with their patient if appropriate. In these areas, health department staff always obtain permission from the HIV-infected individuals physician before contacting the person directly.

Attachment H

Security and Confidentiality Program Requirement Checklist

State: _____ Site: _____

Person completing form _____ Date: _____

Guiding Principles

- Guiding Principle 1** HIV/AIDS surveillance information and data will be maintained in a physically secure environment. Refer to sections [Physical Security](#) and [Removable and External Storage Devices](#).
- Guiding Principle 2** Electronic HIV/AIDS surveillance data will be held in a technically secure environment, with the number of data repositories and individuals permitted access kept to a minimum. Operational security procedures will be implemented and documented to minimize the number of staff that have access to personal identifiers and to minimize the number of locations where personal identifiers are stored. Refer to sections [Policies](#), [Training](#), [Data Security](#), [Access Control](#), [Laptops and Portable Devices](#), and [Removable and External Storage Devices](#).
- Guiding Principle 3** Individual surveillance staff members and persons authorized to access case-specific information will be responsible for protecting confidential HIV/AIDS surveillance information and data. Refer to sections [Responsibilities](#), [Training](#), and [Removable and External Storage Devices](#).
- Guiding Principle 4** Security breaches of HIV/AIDS surveillance information or data will be investigated thoroughly, and sanctions imposed as appropriate. Refer to section [Security Breaches](#).
- Guiding Principle 5** Security practices and written policies will be continuously reviewed, assessed, and as necessary, changed to improve the protection of confidential HIV/AIDS surveillance information and data. Refer to sections [Policies](#) and [Attachment H](#).

Requirements

(Initial items as completed)

- ___ **Requirement 1:** Policies must be in writing. (GP-2)
- ___ **Requirement 2:** A policy must name the individual who is the Overall Responsible Party (ORP) for the security system. (GP-2)
- ___ **Requirement 3:** A policy must describe methods for the review of security practices for HIV/AIDS surveillance data. Included in the policy should be a requirement for an ongoing review of evolving technology to ensure that data remain secure. (GP-5)
- ___ **Requirement 4:** Access to and uses of surveillance information or data must be defined in a data release policy. (GP-2)
- ___ **Requirement 5:** A policy must incorporate provisions to protect against public access to raw data or data tables that include small denominator populations that could be indirectly identifying. (GP-2)
- ___ **Requirement 6:** Policies must be readily accessible by any staff having access to confidential surveillance information or data at the central level and, if applicable, at noncentral sites. (GP-2)
- ___ **Requirement 7:** A policy must define the roles for all persons who are authorized to access what specific information and, for those staff outside the surveillance unit, what standard procedures or methods will be used when access is determined to be necessary. (GP-2)
- ___ **Requirement 8:** All authorized staff must annually sign a confidentiality statement. Newly hired staff must sign a confidentiality statement before access to surveillance data is authorized. The new employee or newly authorized staff must show the signed confidentiality statement to the grantor of passwords and keys before passwords and keys are assigned. This statement must indicate that the employee understands and agrees that surveillance information or data will not be released to any individual not granted access by the ORP. The original statement must be held in the employee's personnel file and a copy given to the employee. (GP-2)
- ___ **Requirement 9:** A policy must outline procedures for handling incoming mail to and outgoing mail from the surveillance unit. The amount and sensitivity of information contained in any one piece of mail must be kept to a minimum. (GP-2)
- ___ **Requirement 10:** In compliance with CDC's cooperative agreement requirement, the ORP must certify annually that all program requirements are met. (GP-2)

- ___ **Requirement 11:** Each member of the surveillance staff and all persons described in this document who are authorized to access case-specific information must be knowledgeable about the organization's information security policies and procedures. (GP-3)
- ___ **Requirement 12:** All staff who are authorized to access surveillance data must be responsible for challenging those who are not authorized to access surveillance data. (GP-3)
- ___ **Requirement 13:** All staff who are authorized to access surveillance data must be individually responsible for protecting their own workstation, laptop, or other devices associated with confidential surveillance information or data. This responsibility includes protecting keys, passwords, and codes that would allow access to confidential information or data. Staff must take care not to infect surveillance software with computer viruses and not to damage hardware through exposure to extreme heat or cold. (GP-3)
- ___ **Requirement 14:** Every individual with access to surveillance data must attend security training annually. The date of training must be documented in the employee's personnel file. IT staff and contractors who require access to data must undergo the same training as surveillance staff and sign the same agreements. This requirement applies to any staff with access to servers, workstations, backup devices, etc. (GP-3)
- ___ **Requirement 15:** All physical locations containing electronic or paper copies of surveillance data must be enclosed inside a locked, secured area with limited access. Workspace for individuals with access to surveillance information must also be within a secure locked area. (GP-1)
- ___ **Requirement 16:** Paper copies of surveillance information containing identifying information must be housed inside locked filed cabinets that are inside a locked room. (GP-1)
- ___ **Requirement 17:** Each member of the surveillance staff must shred documents containing confidential information before disposing of them. Shredders should be of commercial quality with a crosscutting feature. (GP-3)
- ___ **Requirement 18:** Rooms containing surveillance data must not be easily accessible by window. (GP-1)
- ___ **Requirement 19:** Surveillance information must have personal identifiers removed (an analysis dataset) if taken out of the secured area or accessed from an unsecured area. (GP-1)

- ___ **Requirement 20:** An analysis dataset must be held securely by using protective software (i.e., software that controls the storage, removal, and use of the data). (GP-1)
- ___ **Requirement 21:** Data transfers and methods for data collection must be approved by the ORP and incorporate the use of access controls. Confidential surveillance data or information must be encrypted before electronic transfer. Ancillary databases or other electronic files used by surveillance also need to be encrypted when not in use. (GP-1)
- ___ **Requirement 22:** When case-specific information is electronically transmitted, any transmission that does not incorporate the use of an encryption package meeting the Advanced Encryption Standard (AES) encryption standards and approved by the ORP must not contain identifying information or use terms easily associated with HIV/AIDS. The terms HIV or AIDS, or specific behavioral information must not appear anywhere in the context of the communication, including the sender and/or recipient address and label. (GP-2)
- ___ **Requirement 23:** When identifying information is taken from secured areas and included on line lists or supporting notes, in either electronic or hard copy format, these documents must contain only the minimum amount of information necessary for completing a given task and, where possible, must be coded to disguise any information that could easily be associated with HIV or AIDS. (GP-1)
- ___ **Requirement 24:** Surveillance information with personal identifiers must not be taken to private residences unless specific documented permission is received from the surveillance coordinator. (GP-1)
- ___ **Requirement 25:** Prior approval must be obtained from the surveillance coordinator when planned business travel precludes the return of surveillance information with personal identifiers to the secured area by the close of business on the same day. (GP-1)

- ___ **Requirement 26:** Access to any surveillance information containing names for research purposes (that is, for other than routine surveillance purposes) must be contingent on a demonstrated need for the names, an Institutional Review Board (IRB) approval, and the signing of a confidentiality statement regarding rules of access and final disposition of the information. Access to surveillance data or information without names for research purposes beyond routine surveillance may still require IRB approval depending on the numbers and types of variables requested in accordance with local data release policies. (GP-1)
- ___ **Requirement 27:** Access to any secured areas that either contain surveillance data or can be used to access surveillance data by unauthorized individuals can only be granted during times when authorized surveillance or IT personnel are available for escort or under conditions where the data are protected by security measures specified in a written policy and approved by the ORP. (GP-1)
- ___ **Requirement 28:** Access to confidential surveillance information and data by personnel outside the surveillance unit must be limited to those authorized based on an expressed and justifiable public health need, must not compromise or impede surveillance activities, must not affect the public perception of confidentiality of the surveillance system, and must be approved by the ORP. (GP-1)
- ___ **Requirement 29:** Access to surveillance information with identifiers by those who maintain other disease data stores must be limited to those for whom the ORP has weighed the benefits and risks of allowing access and can certify that the level of security established is equivalent to the standards described in this document. (GP-2)
- ___ **Requirement 30:** Access to surveillance information or data for nonpublic health purposes, such as litigation, discovery, or court order, must be granted only to the extent required by law. (GP-2)
- ___ **Requirement 31:** All staff who are authorized to access surveillance data must be responsible for reporting suspected security breaches. Training of nonsurveillance staff must also include this directive. (GP-3)
- ___ **Requirement 32:** A breach of confidentiality must be immediately investigated to assess causes and implement remedies. (GP-4)

- ___ **Requirement 33:** A breach that results in the release of private information about one or more individuals (breach of confidentiality) should be reported immediately to the Team Leader of the Reporting, Analysis, and Evaluation Team, HIV Incidence and Case Surveillance Branch, DHAP, NCHSTP, CDC. CDC may be able to assist the surveillance unit dealing with the breach. In consultation with appropriate legal counsel, surveillance staff should determine whether a breach warrants reporting to law enforcement agencies. (GP-4)
- ___ **Requirement 34:** Laptops and other portable devices (e.g., personal digital assistants [PDAs], other handheld devices, and tablet personal computers [PCs]) that receive or store surveillance information with personal identifiers must incorporate the use of encryption software. Surveillance information with identifiers must be encrypted and stored on an external storage device or on the laptop's removable hard drive. The external storage device or hard drive containing the data must be separated from the laptop and held securely when not in use. The decryption key must not be on the laptop. Other portable devices without removable or external storage components must employ the use of encryption software that meets federal standards. (GP-1)
- ___ **Requirement 35:** All removable or external storage devices containing surveillance information that contains personal identifiers must:
- (1) include only the minimum amount of information necessary to accomplish assigned tasks as determined by the surveillance coordinator,
 - (2) be encrypted or stored under lock and key when not in use, and
 - (3) with the exception of devices used for backups, devices should be sanitized immediately following a given task. Before any device containing sensitive data is taken out of the secured area, the data must be encrypted. Methods for sanitizing a storage device must ensure that the data cannot be retrievable using Undelete or other data retrieval software. Hard disks that contained identifying information must be sanitized or destroyed before computers are labeled as excess or surplus, reassigned to nonsurveillance staff, or before they are sent off-site for repair. (GP-1)

MEMORANDUM

Date:

From: (Principal Investigators)

Subject: Request of Waiver of Documentation of Informed Consent, Protocol (#)

To: Human Subjects Committee

We submit for your review a request to waive documentation of informed consent for protocol (#) entitled “National HIV Behavioral Surveillance among men who have sex with men (NHBS-MSM3).” We request a waiver of documentation of informed consent as provided in the second criterion (below) under Federal Regulations Title 46, Section 117, Documentation of Informed Consent, paragraph (c):

An IRB may waive the requirement for the investigator to obtain a signed informed consent for some or all subjects if it finds either:

- (1) That the only record linking the subject and the research would be the consent document and the principal risk would be the potential harm resulting from a breach of confidentiality. Each subject would be asked whether the subject wants documentation linking the subject with the research, and the subject’s wishes will govern; or*
- (2) That the research presents no more than minimal risk of harm to subjects and involves no procedures for which written consent is normally required outside of the research context.*

Protocol (#) presents no more than minimal risk of harm to subjects. Participation involves the completion of an anonymous interviewer-administered risk behavior questionnaire and a voluntary HIV counseling and testing component.

Appendix N Consent

Required Elements of Informed

The Code of Federal Regulations for the Protection of Human Subjects, Section §46.116, describes eight elements required in each consent process/document. Element number six is only required if the research is determined to be greater than minimal risk.

Element	45 CFR 46.116(a)
1.	A. a statement that the study involves research
	B. an explanation of the purposes of the research
	C. the expected duration of the subject's participation
	D. a description of the procedures to be followed
	E. identification of any procedures which are experimental
2.	a description of any reasonably foreseeable risks or discomforts to the subject
3.	a description of any benefits to the subject or to others which may reasonably be expected from the research
4.	a disclosure of appropriate alternative procedures or courses of treatment, if any, that might be advantageous to the subject
5.	a statement describing the extent, if any, to which confidentiality of records identifying the subject will be maintained
6.	A. an explanation as to whether any compensation is available if injury occurs
	B. an explanation as to whether any medical treatments are available if injury occurs, and, if so
	C. what they consist of or where further information may be obtained
7.	A. an explanation of whom to contact for answers to pertinent questions about the research
	B. an explanation of whom to contact for answers to pertinent questions about the research subjects' rights
	C. whom to contact in the event of a research-related injury to the subject
8.	A. a statement that participation is voluntary
	B. refusal to participate will involve no penalty or loss of benefits to which the subject is otherwise entitled
	C. the subject may discontinue participation at any time without penalty or loss of benefits to which the subject is otherwise entitled