NCHS Confidentiality Practices
for Federal Employees and Contractors

Hello. My name is Al Zarate. I'm the NCHS Confidentiality Officer.

In a recent period, the Center made pledges of confidentiality to more than 3/4 of a million persons, close to 50,000 hospitals and nursing homes, and some 18,000 physicians.

The assurance of confidentiality, however, is just the beginning. NCHS does everything it can to insure that these promises will actually be kept.

That's what this presentation is all about. Not only is living up to our guarantee good statistical practice, it happens to be the right thing to do - and it's required by law.

Anyone paying any attention to the news these days knows that there is a very serious public concern with issues of privacy and confidentiality. This is particularly true of the health field where the demand for information on the cost and financing of health care as well as health conditions and their causes and treatment has led to the collection of more and more information - often of a "sensitive" nature.

All of this means that there is even more pressure now to promise, and deliver, *strict* confidentiality.

NCHS has never had an actual or even an alleged breach of confidentiality. This is not an accident. Our record is based upon the continued observation and improvement of carefully considered policy and practices. It does not require much imagination to realize that even the *appearance* of a violation of even *one* respondent's privacy would seriously impair NCHS' function as a statistical agency. Inattention to this most serious matter could cause irreparable personal harm and damage or destroy the integrity of NCHS and its agents.

For these reasons NCHS must do all it can to insure that its employees and contractors protect the privacy of our respondents.

A Confidentiality package has been prepared for each of you, containing:

- A special summary guide to the NCHS Confidentiality Manual
- A copy of the NCHS Non-Disclosure form that you are all required to sign upon assuming your positions.
- A list of Do's and Don'ts which summarize the most important actions concerning confidentiality that you need to take or avoid.
- A list of the most commonly asked questions concerning confidentiality (with answers), and
- A list of Do's and Don'ts concerning electronic security.

Reviewing these documents is not optional. You are *required* to be familiar with their contents – particularly those of the Confidentiality Manual.

Today, I'd like to talk about:

- The meaning of the term "confidentiality"
- The significance of the non disclosure form
- Steps that we must all take
- Actions that we must positively avoid

Simply put, confidential information is <u>information provided with a restriction concerning who else would know about it</u>.

At NCHS this term is reserved for information that can be associated with a person or establishment – that is, information which is "identifiable" and whose release outside the agreed upon restrictions would constitute a confidentiality "breach".

When the Center provides an assurance of confidentiality, that assurance represents a pledge that ANY information a person provides which could be associated with them personally will not be released to anyone other than those they've agreed to.

This assurance is provided in somewhat different ways in each of our data collection systems, but the following statement gives the essence of what we promise:

"We will hold all data we collect in the strictest confidence. We gather and protect all data in keeping with the requirements of Federal Laws:" … (which) "prohibit us from giving out information that identifies you or your

family without your consent. This means that we cannot give out any fact about you, even if a court of law asks for it…" (NHANES 2005)

It is NCHS practice to provide for the release of identifiable information to other parties such as contractors or other government agencies by clearly informing respondents as to who will be granted access to identifiable data, and for what purpose, *before* the respondent decides whether to participate in one of our surveys.

After that we are legally and ethically BOUND by that statement.

If we tell respondents that no one but NCHS staff and contractors will see identifiable information, we are then <u>not</u> able to share that information even within our parent organization (CDC), let alone the rest of the Department of Health and Human Services. On the other hand, we are permitted to share such data even with agencies outside of the Department as long as the intention to do so has been clearly stated to respondents. When we do, we are very careful to make sure that the confidentiality of records that we share is in no way jeopardized.

Each of you must sign a non-disclosure "pledge" or affidavit indicating that you are aware that divulging confidential information is punishable by law. You will be asked to sign this same pledge annually during your tenure at NCHS. Please note that punishment for knowingly violating Federal law can include conviction of a felony, jail, loss of job, and a fine of up to $250,000.

As strong of a deterrent as these legal sanctions are, the consequences of unethical behavior for ones' professional reputation are equally severe.

Because of its very serious nature, I urge you to take the opportunity to read it carefully and to raise any questions you might have with your supervisor or with me.

Also part of your packet is an executive summary of the NCHS Confidentiality Manual. The Manual is the authoritative statement of NCHS policy concerning all matters related to confidentiality. You are required to be familiar with the complete Manual found at the websites listed on the summary. The summary is intended as a handy guide to the Manual to be used when you have a specific question or concern. Please read it carefully. You are responsible for knowing its contents.

Some of you are survey statisticians, epidemiologists or demographers. Others are coding clerks, administrative officers, support staff or program analysts. You may be seeing this presentation here in Hyattsville, at NCHS offices in North Carolina or elsewhere.

Whatever your job classification or type of appointment, and wherever you perform your function or assignment, if you work with identifiable data, *these requirements apply to you.* LET ME REPEAT THAT …

Whatever your job classification or type of appointment, and wherever you perform your function or assignment, if you work with identifiable data, *these requirements apply to you.*

Even if we're not dealing with so-called "sensitive" information, the requirements would apply if the data are included with *other* information which are personally identifiable. What kind of data are we talking about? Well, here are *some* examples.

Aside from the obvious items such as name, address and SSN, a number of details could be used to deduce or infer a person's identity, particularly if a person happens to have a rare or highly visible characteristic or some condition or combination of characteristics makes them stand out.

This cartoon shows what can happen even if names are deleted; the remaining information, if it can be matched with similar information, can "lead" to identification. Here, in spite of the mask, and the elimination of his name, we can still determine what the bank robber must look like and are in a position to learn his name.

It is very important to recognize that these confidentiality requirements apply to administrative as well as to statistical information. They are not limited to data collected in our surveys, but apply as well to information we ourselves provide relating to our employment at NCHS.

As you can see, this involves many documents and files that we are accustomed to fill out and access on a regular basis.

At whatever stage of data processing – collection, coding, editing, trashing or recycling - and in whatever form records are kept - if there is a name or social security number on it, it must be treated with utmost care.

This applies as well to papers we present at professional meetings and elsewhere.

Whether it is:

- an interview form with a name or address on it,
- a microfilm of a death certificate with the name of the deceased, attending physician, or informant, or
- a travel document or leave slip containing name and social security number,

it must be treated as confidential.

This means that you should never:

- Mail, fax, or send confidential material in electronic form to other NCHS staff, contractors of other Federal agencies without observing strict security procedures,
- Search through a file to see if your neighbor or an acquaintance might have been interviewed in one of our surveys or seek in any way to use any information you may find for any purpose.
- Discuss in public any identified person's or institution's participation in an NCHS survey.

In addition, you should never,

- Leave confidential records in places visible to unauthorized persons.
- Prepare or maintain unneeded copies of confidential material.

It is also very important that you do not:

- Remove confidential documents or files from NCHS offices for any purpose (including taking them home to work on laptops, compact disks or flash drives) or access them electronically from an unauthorized remote location.

Also, do not assume e-mail communications are safe. They are not secure.

- Finally, without our respondent's consent, the law prohibits releasing identifiable information to other Federal agencies (even within CDC),

with funding agencies, collaborators and even with Congressional subcommittees, or in response to a judicial subpoena. Without first having obtained our respondent's permission to do so. We CANNOT release identifiable data to any of these parties.

The NCHS law takes precedence even over judicial subpoenas, Freedom of Information Inquiries and Presidential order and it has been upheld in Federal court.

So, before you answer any request for identifiable data, check with your supervisor, or with me.

Further examples and details are provided in the questions and answers and Do's and Don'ts. Please review them at your earliest opportunity.

Ultimately, it's not a "system" or the signing of a pledge that protects our confidential data. It's people like you doing their job responsibly and with respect for the people who provide us insights into their private lives.

We're depending on you.

Thank you.