



**NATIONAL HEALTHCARE SAFETY NETWORK
FACILITY/GROUP USER & ADMINISTRATOR
RULES OF BEHAVIOR**

Version 3.0

06/12/2019

VERSION HISTORY

Version #	Implemented By	Revision Date	Reason
1.0	James Tolson	08/08/2005	
2.0	Katherine Danner	08/28/2012	Update document to reflect change to Secure Access Management Services (SAMS)
3.0	Muzna Mirza	06/12/2019	Updated based on changes to NHSN purposes as reflected in the updated 'Agreement to participate and consent' signed by NHSN Users during 2017 and 2018

TABLE OF CONTENTS

1 INTRODUCTION.....	4
1.1 Purpose	4
1.2 Definitions	4
1.2.1 What are the Rules of Behavior?	4
1.2.2 Who is covered by these Rules?	5
1.2.3 What are Penalties for Non-compliance?	5
2 POLICY RULES.....	5
2.1 Legal, Regulatory, and Policy Requirements	5
2.2 Statement of System Policy.....	5
3 USER RESPONSIBILITIES	6
3.1 Ethical Conduct	6
3.2 Authentication Management	6
3.3 Information Management and Document Handling.....	7
3.4 NHSN SYSTEM ACCESS AND USAGE	7
3.4.1 Healthcare Facility Users of NHSN.....	7
3.4.2 Group Users of NHSN	8
3.4.3 Security responsibilities	9
3.4.4 Training.....	10
3.4.5 Prohibitions	11
4 USER ASSISTANCE AND ADDITIONAL RESOURCES.....	11
5 REVISIONS AND RENEWAL	11
6 ACKNOWLEDGEMENT AND AGREEMENT	11
7 APPENDIX-A.....	13
7.1.1 References.....	13

1 INTRODUCTION

The National Healthcare Safety Network (NHSN) is a surveillance system that is developed, maintained, and used by the Centers for Disease Control and Prevention (CDC). NHSN enables participating healthcare facilities to submit and analyze data on patient and healthcare worker safety, such as surgical site infections, antimicrobial use and resistance, bloodstream infections, blood safety incidents, dialysis incidents, and healthcare worker vaccinations. It provides analysis tools that enable NHSN Users to generate a variety of reports, many of which use data aggregated by NHSN for benchmarking purposes. Healthcare facilities, state and local health departments, and other NHSN Users use these resources to identify prevention and quality improvement opportunities and track progress in efforts to prevent adverse healthcare events and enhance patient and healthcare worker safety. NHSN also provides links to best practices, guidelines, and lessons learned.

NHSN collects, processes, stores, and makes accessible to authorized users a large volume of sensitive patient and healthcare facility data. These data must be protected from unauthorized access, disclosure, or modification in accordance with a comprehensive set of confidentiality, privacy, integrity, and availability requirements. The loss, misuse, or unauthorized access to or modification of data in the system could result in a loss of confidentiality and privacy. The resulting adverse effect on the integrity of NHSN data would also negatively impact decision-making and scientific data analysis.

1.1 PURPOSE

To safeguard against unwarranted or inadvertent misuse or disclosure of NHSN data, each NHSN User must abide by NHSN's Rules of Behavior. This document is a comprehensive description of the NHSN Rules of Behavior that apply to all Users of the NHSN web-based computer system, including NHSN Users at CDC and the Users who gain access to NHSN data remotely.

1.2 DEFINITIONS

1.2.1 What are the Rules of Behavior?

Rules of Behavior are a comprehensive set of requirements that govern Users' interactions with an information system and their use of system data. The NHSN Rules of Behavior are developed, maintained, and promoted by CDC staff who have lead responsibilities for NHSN operations. Their goals for the NHSN Rules of Behavior are to inform NHSN Users of the system's requirements and to assure that all patient- and facility-identifiable data reported to NHSN are safeguarded against unwarranted or unauthorized uses or disclosures. The NHSN Rules of Behavior are predicated on the guiding principles that knowledgeable Users are the foundation of a successful information system security program, and clearly defined and well described set of rules are an essential part of imparting and applying knowledge of security safeguards. Each NHSN User must fully understand and abide by these rules in their interactions with the system and their use of system data.

1.2.2 Who is covered by these Rules?

These rules apply to each User who seeks and gains access to the NHSN system. These rules extend to CDC NHSN team members and their authorized contractors and agents (such as guest researchers, students) and to all NHSN Users, including NHSN Facility and/or Group Administrators. Each NHSN User is responsible for understanding and abiding by the Rules of Behavior and will be held accountable for their actions involving NHSN data in accordance with the rules.

1.2.3 What are Penalties for Non-compliance?

Compliance with the NHSN Rules of Behavior is of the utmost importance. Non-compliance will be addressed through sanctions imposed under existing policy and regulation. Sanctions will be appropriate with the level of infraction and can include a written or verbal warning and possible suspension or cessation of system access privileges.

2 POLICY RULES

2.1 LEGAL, REGULATORY, AND POLICY REQUIREMENTS

The security requirements of the NHSN application hosted by CDC are grounded in CDC's commitment to safeguard against unauthorized access and use of NHSN data. CDC assures that its use of data that the healthcare facilities submit to NHSN, including CDC's disclosures of facility-identifiable data, is limited to the NHSN purposes <https://www.cdc.gov/nhsn/about-nhsn/technology.html>. These NHSN purposes are specified in the NHSN Agreement to Participate and Consent Form, which is reviewed and signed by designated personnel at each participating facility. This form is a legal document, and CDC is legally bound to adhere to its provisions.

The NHSN Rules of Behavior are derived largely from legal requirements and guidelines promulgated by Department of Health and Human Services (HHS) and other Federal document sources, most specifically OMB Circular A-130, Subsection (m) of the Privacy Act of 1974 (U.S.C. 552a) and Section 308(d) of the Public Health Service Act (U.S.C. 242m). See Appendix A for more information. The NHSN Rules of Behavior are in large part based on stipulations and guidance provided by the directives, publications and programs in Appendix-A.

2.2 STATEMENT OF SYSTEM POLICY

Users are provided access to NHSN through the CDC's Secure Access Management Services (SAMS) for the purpose of facilitating CDC's public health mission. CDC maintains security for all systems accessible through SAMS, therefore CDC has the authority under federal law to monitor all Users' communications on SAMS, even with remote equipment. This statutory authority is based on the need for ensuring the appropriateness of such communications, and for that purpose random computer checks are needed. CDC's SAMS and NHSN system management may periodically monitor both

systems and User activities for purposes including, but not limited to, troubleshooting, performance assessment, usage patterns, indications of attack or misuse and the investigation of complaints or suspected security incidents.

3 USER RESPONSIBILITIES

3.1 ETHICAL CONDUCT

The NHSN database includes a large volume and variety of sensitive data. This sensitive data requires protection from unauthorized access, disclosure, or modification based on confidentiality, integrity, and availability requirements. To safeguard data integrity, confidentiality and privacy, scrupulous attention to safe data management policies and practices is essential.

All system Users are responsible for:

- Taking every reasonable precaution to ensure that all patient and/or healthcare facility-identifiable data accessed via NHSN is used solely for authorized analytic purposes and is not intentionally or inadvertently disclosed in any way that breaches the confidentiality provisions of the NHSN Agreement to Participate and Consent Form completed by each healthcare facility that participates in NHSN
- Removing patient and/or healthcare facility identifiers when presenting data for discussion with individuals who do not have authorized access to those data
- Accessing or using sensitive patient- or facility identifying information only when necessary to perform job functions, and not accessing or using sensitive information for anything other than authorized purposes
- Informing Facility or Group Administrators about any change in their role and/or employment status which would require change in their NHSN system access permissions
- Self-managing their access and stop accessing NHSN data for any healthcare facility for which they no longer have a surveillance or related role

Administrative Users understand that as privileged Users they must:

- Not share privileged User account(s), password(s)/passcode(s)/grid cards, PINs and other login credentials
- Not access information outside of the scope of specific job responsibilities or expose non-public information to unauthorized individuals

3.2 AUTHENTICATION MANAGEMENT

Users must access NHSN through the SAMS partner portal. SAMS requires an identity proofing process, and Users approved for NHSN access will receive instructions on the SAMS identity proofing process.

It is incumbent on all NHSN Users to:

- Ensure the security of their SAMS password and grid card (if applicable). System administrators will never ask for your password and cannot retrieve your password for you
- Immediately inform the SAMS Help Desk at samshelp@cdc.gov if they are concerned or know that their SAMS password and/or grid card have been compromised in any way.

3.3 INFORMATION MANAGEMENT AND DOCUMENT HANDLING

Hard copy documents (e.g., reports, print-outs), as well as electronic data and information, should be safeguarded against unwarranted access or disclosure. Such protection is in accordance with the assurance of confidentiality that CDC affords to healthcare facilities that participate in NHSN and in accordance with federal data and information system security, privacy and confidentiality regulations, policies and statutes. (See references)

Specifically, the Users must:

- Not save NHSN data on portable storage media such as on flash drives and laptop computers or on local hard drives. System data may be stored on institutional information systems that are secured by information technology and security professionals.
- Always access NHSN system on secure computers protected by physical and virtual information security mechanisms.
- Not share NHSN data with Personally Identifiable Information (PII) via email.
- Securely dispose of electronic media and papers that contain sensitive data when no longer needed, in accordance with the HHS Policy for Records Management and federal guidelines.

3.4 NHSN SYSTEM ACCESS AND USAGE

3.4.1 Healthcare Facility Users of NHSN

Facility Administrators

When a healthcare facility enrolls in NHSN, CDC will assign an NHSN facility ID number to the facility and invite the Facility Administrator to register with SAMS for completing NHSN enrollment. For detailed enrollment information, please refer to [SAMS information](#). Facility Administrators are initially given access rights upon activation of their facility in NHSN as the final step of the enrollment process. Facility Administrators have all access rights and can update facility information; add, modify, and delete Users within their facility; reassign the Facility Administrator role; and assign the Users specific roles and access rights. Facility Administrators are responsible for managing and inactivating Users in their facility who no longer have a role related to NHSN surveillance activities for their organization. While each facility enrolled in NHSN can have only one Facility Administrator, administrative rights can also be granted to additional Users.

Facility Users

Users will be added to NHSN by their NHSN Facility Administrator or others with administrative rights. When the User account is added, the User will receive an email containing instructions to register with SAMS for completing NHSN enrollment. Users are assigned roles and accompanying access rights to various parts of the application. The User is responsible for notifying the NHSN Facility Administrator of any changes in job status (such as promotion, demotion, transfer, termination) that might affect the appropriateness of continued access and specific NHSN system rights.

If Users move to another healthcare facility for which they may need to access the NHSN system, they will not need to go through the SAMS process again if they will be using the same email address with which they initially registered with SAMS, and if the new NHSN Facility Administrator or someone with administrative rights grants them access. If change in healthcare facility means a change in User email address, then the new employer's Facility Administrator or someone with administrative rights will need to invite them, and they will need to register with SAMS again.

3.4.2 Group Users of NHSN

NHSN Group Functionality

The NHSN Group functionality is a technical feature within the NHSN application that enables healthcare facilities to join a Group within the NHSN framework to share some or all of their data at a single (Group) level for a mutual purpose with another entity, such as for performance improvement, required reporting and/or data sharing under a Data Use Agreement. Any third party entity (other than the facility and CDC), such as a state or local health department, corporate headquarters for healthcare facilities, or End Stage Renal Disease (ESRD) Network Organization, can maintain a Group in NHSN whereby NHSN becomes the vehicle for sharing data between the Group and the NHSN facility; the relationship is between those two entities. The NHSN Facility Administrator and others with administrative rights have the ability to join the healthcare facility to the Group and confer rights, i.e. provide access to some or all of the data requested by the Group. A facility that joins a Group does not have access to any data from other facilities in the Group, and facilities may join multiple NHSN Groups.

Group Administrators and Group Users

An entity that maintains a Group in NHSN identifies a Group Administrator who communicates regularly with the Group's member facilities. While each Group enrolled in NHSN can have only one Group Administrator, administrative rights can also be granted to additional NHSN Users in the organization. Such Group Users are identified by the Group Administrator and given rights to view and analyze data shared by member facilities in the Group. Group Administrators are responsible for managing and inactivating Users in their Group who no longer have a role related to NHSN surveillance activities for their organization.

Group Users can view and analyze data reported by all facilities in a Group or individual facilities for which they have authorized access. All NHSN Group Users, including Group Administrators, are custodians of the data to which they gain access via the NHSN Group functionality, and they are responsible for establishing, using, and maintaining appropriate administrative, technical, and physical safeguards to prevent unauthorized access or use of the NHSN data to which they have gained access.

NHSN Group Users are responsible for communicating to prospective healthcare facility participants in their Group the Group User's purpose(s), plans for data use, and the safeguards that the Group User will use to protect the confidentiality of the NHSN data to which it seeks access. Healthcare facility users that join NHSN Groups can expect that NHSN Group Users will inform the facilities in their groups in writing if and when the purpose or scope of the groups' analyses change. Additionally, NHSN facility users can expect that opportunities will be provided for facilities to consent or refrain from consenting to use of the groups' NHSN data for the additional analytic use(s).

Find more information on Groups and Group Administrators at <https://www.cdc.gov/nhsn/group-users/index.html>

3.4.3 Security responsibilities

All Users: Awareness and General Incident Reporting

All Users of NHSN system and information shall:

- Be vigilant of and be responsible for reporting suspicious security incidents, any loss, compromise, and unauthorized use of NHSN system and data or of authenticating information, immediately upon discovery/detection in accordance with HHS policies.
- Immediately report any incidents of suspected fraud, waste, or misuse of NHSN system to their NHSN Facility/Group Administrator, in addition to the NHSN Help Desk at nhsn@cdc.gov. When in doubt or if more information is needed, Users are encouraged to contact the NHSN Help Desk at nhsn@cdc.gov
 - Immediate reporting means: Report incidents as soon as possible, without unreasonable delay and no later than within one (1) hour of occurrence/discovery
- Help to prevent unauthorized use of and access to system resources by logging out of the NHSN system and locking the computer screen to prevent unauthorized access and also by physically securing the computer when stepping away. This duty includes complying with all stated policy requirements, taking due care and reasonable precautions when handling system data or using system resources.
- Complete security trainings (such as security and privacy awareness, role-based training) prior to accessing HHS systems and periodically thereafter according to organizational policies.

- Be accountable for their actions while accessing and using NHSN data on HHS information systems and IT resources
- Protect passwords and other access credentials such as grid cards from disclosure and compromise
- Promptly change password when required by system policy and if they suspect that it has been compromised
- Not use another person's account, identity, password/passcode/PIN, or grid card or allow others to use information resources provided to them to perform official work duties and tasks
- Use systems with at least the following protections in place to access sensitive data on HHS information systems:
 - Antivirus software with the latest updates
 - Anti-spyware and personal firewalls
 - A time-out function that requires reauthentication after no more than 30 minutes of inactivity on remote access

Administrators: Security safeguards

Each NHSN Facility and Group Administrator must:

- Ensure that physical, information system and administrative policy safeguards are operational within their areas of responsibility
- Restrict access to NHSN system information and data to authorized personnel on a need to know basis
- Document and investigate known or suspected security incidents or violations (including sharing of grid card) and report them to the CDC through the NHSN Help Desk immediately upon gaining awareness
- Verify that Users have received pertinent security training before allowing them access to NHSN
- Protect all Administrative User account passwords/passcodes/personal identified numbers (PINs) and other login credentials used to access NHSN system
- Comply with all system/network administrator responsibilities in accordance with applicable policies
- Notify system owners immediately when privileged access is no longer required

3.4.4 Training

NHSN training resources are available online at:

- <https://www.cdc.gov/nhsn/training/index.html>
- <https://www.cdc.gov/nhsn/training/enrollment-setup/index.html>
- <https://www.cdc.gov/nhsn/training/roadmap/index.html>

3.4.5 Prohibitions

All system Users shall adhere to the following prohibitions:

- Do not share their security credentials (SAMS password, grid cards).
- Do not attempt to access any data or programs on the NHSN system for which they do not have authorization.
- Sharing of facility-identifiable HAI, Antibiotic Use and Resistance (AUR), blood safety, and healthcare worker influenza vaccination data and any NHSN data with Personally Identifiable Information (PII) via email is strictly prohibited.
- Do not engage in, encourage, or conceal any “hacking” or “cracking,” denial of service, unauthorized tampering, or unauthorized attempted use of or deliberate disruption of any computer system within the NHSN system.
- Do not purposely engage in any activity with the intent to:
 - Degrade the performance of the system
 - Deprive an authorized User access to a resource
 - Obtain or attempt to obtain extra resources beyond those allocated
 - Circumvent security measures in order to gain access to any automated system for which proper authorization has not been granted
- Transporting, transmitting, e-mailing, texting, remotely accessing, or downloading sensitive information unless such action is explicitly permitted in writing by the manager or owner of such information and appropriate safeguards are in place per HHS policies concerning sensitive information.
- Do not knowingly or willingly conceal, remove, mutilate, obliterate, falsify, or destroy system data.

4 USER ASSISTANCE AND ADDITIONAL RESOURCES

To obtain system-related assistance (Help Desk, vendor support, system management, etc.), Users should contact the relevant help desk from the following contact information table:

Name	Email
NHSN Help Desk	nhsn@cdc.gov
SAMS Help Desk	samshelp@cdc.gov

5 REVISIONS AND RENEWAL

When new versions of this document are released, the system business or technical steward will provide a revised copy to all Users. Send comments, feedback, questions, and objections to the NHSN Help Desk.

6 ACKNOWLEDGEMENT AND AGREEMENT

I have read and agree to comply with the terms and conditions governing the appropriate and allowed use of NHSN as defined by this document, applicable agency policy, and Federal law. I understand that infractions of these rules will be considered violations of

CDC standards of conduct and may result in disciplinary action including the possibility of supervisory notification, suspension of system privileges, and/or criminal and civil prosecution.

The act of acknowledgement and agreement signifies a clear understanding of the NHSN Rules of Behavior document and that the signer will conform to the rules provided therein.

I acknowledge receipt of, understand my responsibilities, and will comply with the rules of behavior for NHSN.

Signature

Date

Printed Name

7 APPENDIX-A

The NHSN Rules of Behavior are in large part based on stipulations and guidance provided by the following directives, publications, and programs and as referenced in References below:

1. HHS Rules of Behavior for the Use of HHS Information and IT Resources Policy
2. Office of Management and Budget (OMB) Circular A-130
3. National Institutes of Health (NIH) Information Technology General Rules of Behavior
4. Privacy Act of 1974
5. Freedom of Information Act
6. Section 508 of the Workforce Investment Act of 1998
7. Computer Security Act Public Law 100-235
8. E-Government Act Public Law 107-347
9. Paperwork Reduction Act of 1995
10. Clinger-Cohen Act of 1996
11. Secure Access Management Services (SAMS)
12. National Institute of Standards and Technology (NIST) publications
13. Health Insurance Portability and Accountability Act of 1996 (HIPAA)
14. Human and Human Services Automated Information Systems Security Program (HHS AISSP) Handbook

7.1.1 References

- [1] Health and Human Services (HHS) Rules of Behavior for the Use of HHS Information and IT Resources Policy. Accessed online on March 12, 2019
<https://www.hhs.gov/web/governance/digital-strategy/it-policy-archive/hhs-rules-of-behavior-for-the-use-of-hhs-information-and-it-resources-policy.html>
- [2] Office of Management and Budget. Circular No. A-130, Revised, (Transmittal Memorandum No. 4): Management of Federal Information Resources. Accessed online on March 6, 2019.
<https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130trans4.pdf>
- [3] Center for Information Technology, National Institutes of Health, NIH Information Technology General Rules of Behavior. Accessed online on March 6, 2019.
https://ocio.nih.gov/aboutus/publicinfosecurity/securitytraining/Pages/NIH_IT_GeneralRulesofBehavior.aspx
- [4] The Privacy Act of 1974, 5 USC § 552a. Accessed online on March 6, 2019.
<https://www.justice.gov/opcl/privacy-act-1974>
- [5] The Freedom of Information Act 5 U.S.C. § 552, As Amended By Public Law No. 104-231, 110 Stat. 3048. Accessed online on March 6, 2019.
http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm

-
- [6] Section 508 of the Workforce Investment Act of 1998. Accessed online on March 6, 2019. <https://www.justice.gov/sites/default/files/crt/legacy/2009/02/18/508law.pdf>
- [7] Computer Security Act Public Law 100-235. Accessed online on March 6, 2019. <https://www.gpo.gov/fdsys/pkg/STATUTE-101/pdf/STATUTE-101-Pg1724.pdf>
- [8] E-Government Act Public Law 107-347. Accessed online on March 6, 2019. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107
- [9] Paperwork Reduction Act of 1995. Accessed online on March 6, 2019. <https://www.gpo.gov/fdsys/pkg/PLAW-104publ13/content-detail.html>
- [10] Clinger-Cohen Act of 1996. Accessed online on March 6, 2019. <https://dodcio.defense.gov/Portals/0/Documents/ciodesrefvolone.pdf>
- [11] Secure Access Management Services (SAMS). Accessed online on March 6, 2019. <https://www.cdc.gov/nhsn/sams/about-sams.html>
- [12] National Institute of Standards and Technology (NIST) publications. Accessed online on August 8, 2018. <https://www.nist.gov/publications>
- [13] Health Insurance Portability and Accountability Act of 1996 (HIPAA). Accessed online on March 6, 2019. <https://www.hhs.gov/hipaa/index.html>
- [14] HHS Automated information systems security program (AISSP) handbook. Accessed online on March 6, 2019. <https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir4636.pdf>