

## **Occupational Health Safety Network (OHSN) Rules of Behavior**

### **February 2016**

#### **Introduction**

OHSN is a voluntary and secure electronic occupational safety and health surveillance system maintained by the National Institute for Occupational Safety and Health (NIOSH), part of the Centers for Disease Control and Prevention (CDC). OHSN processes and stores a variety of sensitive data. This information requires protection from unauthorized access, disclosure, or modification based on confidentiality, integrity, and availability requirements. These “Rules of Behavior” apply to all users of the OHSN web-based computer system, including Healthcare System & Facility Administrators, Report Users, and NIOSH OHSN team members and their authorized contractors and agents (e.g., guest researchers, students).

#### **Purpose**

The rules of behavior are not to be used in place of existing policy; rather they are intended to enhance and further define the specific rules each user must follow while accessing and using OHSN. The rules are consistent with the policy and procedures described in the [Department of Health and Human Services \(DHHS\) Information Security and Privacy Program](#) and specific policy documents. The DHHS Information Security and Privacy program contains computer security guidance on a wide range of topics and describe the Information Technology Security Program that establishes policies, procedures, and responsibilities in the area of computer security within the Department.

#### **Non-compliance**

Non-compliance with these rules will be enforced through sanctions appropriate with the level of infraction. Actions may range from a verbal or written warning and/or removal of system access depending on the severity of the violation.

#### **Policy Rules**

Information handled by the system includes sensitive information. The loss, misuse, or unauthorized access to or modification of information in the system could result in a loss of confidentiality, integrity, and availability of the system data. If integrity of OHSN data were adversely affected, it would negatively impact decision-making and scientific data analysis.

**OHSN does not collect personally identifiable information (PII). CDC/NIOSH asks users not to include PII in any OHSN records.**

Users are provided access to OHSN for the purpose of facilitating CDC/NIOSH’s public health mission. Each user is responsible for helping to prevent unauthorized use of, and access to, system resources. This duty includes complying with all stated policy requirements, taking due

care and reasonable precautions when handling system data or using system resources, and in managing and protecting system authentication controls (passwords, etc.). When in doubt, users are strongly encouraged to contact OHSN Help by sending an email to [NIOSHOSHNS@CDC.gov](mailto:NIOSHOSHNS@CDC.gov) or calling 513-841-4337.

Users shall not attempt to access any data or programs on the OHSN system for which they do not have authorization.

Users shall 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 OHSN system.

Users shall 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
- Falsify records

Users will access OHSN through an OHSN user account and password authentication. Each OHSN user will have a unique user name and password for the system.

Each user is responsible for protecting his/her password. Passwords should not be shared as users are responsible for all actions performed with their account. Users who believe their password has been compromised in any way will immediately inform OHSN. Users will supply a password that meets the OHSN requirements. (Passwords must be at least eight characters in length and must contain at least one capital letter, one lower case letter, and no spaces. The maximum number of characters in the password is 30.)

NIOSH OHSN System Administrators may periodically monitor both the system and user activities for purposes including, but not limited to, troubleshooting, performance assessment, usage patterns, indications of attack or misuse and the investigation of a complaint or suspected security incident.

## OHSN Healthcare Modules – Roles and Responsibilities

The Healthcare Modules of OHSN provide different user roles. Each role provides different levels of data access. A user can be assigned more than one role. Users are assigned roles and accompanying access rights to various parts of the application by their Healthcare System or Facility Administrator. Roles include:

- Healthcare System Administrators
- Facility Administrators
- Healthcare System Report Users
- Facility Report Users

All OHSN Users must:

- Notify the Healthcare System or Facility Administrator of changes in job status that might affect the appropriateness of continued access.
- Comply with all items in the OHSN Rules of Behavior

**Healthcare Facility Administrator Role:** Facility Administrators have rights to view and access data and user information within their healthcare *facility*. A healthcare facility may or may not belong to a healthcare *system*. Healthcare Facility Administrators can update only their own facility information and can request adding, modifying, or deleting users only within their facility, as well as assign users specific roles and access rights.

**Healthcare System Administrator Role:** System Administrators have rights to view and access data and user information within their healthcare *system*. A healthcare system is made up of two or more healthcare facilities. Healthcare System Administrators can update individual facility information for facilities within their system and can request adding, modifying, or deleting users within their system, as well as assign users specific roles and access rights.

### Additional Responsibilities for Healthcare System & Facility Administrators

Healthcare System and Facility Administrators should be vigilant for and have responsibility for reporting suspicious events, system misuse, suspected compromise or loss of data. Administrators should report such instances immediately to NIOSH OHSN System Administrator by sending an email to [NIOSHOHSN@CDC.gov](mailto:NIOSHOHSN@CDC.gov) or calling 513-841-4337.

Healthcare System and Facility Administrators have added responsibilities to ensure the secure operation of OHSN:

- Ensure that adequate physical and administrative safeguards at the facility are operational within their areas of responsibility and that access to information and data is restricted to authorized personnel
- Ensure users have received appropriate training before allowing access to OHSN. Training will be coordinated with NIOSH at the time of enrollment.

- Document and investigate known or suspected security incidents or violations and report them to the OHSN system administrators as soon as detected
- Ensure that the denominator data for their facility is accurate
  - Denominator data must be reviewed and updated at least once a year
  - Denominator data should be updated whenever a major expansion or contraction of services occurs

Healthcare System Administrators must ensure that only facilities owned by the healthcare system participate in OHSN as a system member. Facilities affiliated in any other way must enroll separately.

**Healthcare Facility or System Administrators** are responsible for uploading the most accurate and timely data possible to the OHSN system. They must:

- Submit only real data, not test data, to the OHSN production system
- Properly code OHSN data elements according to the OHSN Standardized Occupational Data Architecture (SODA)
- NOT include any personally identifying information in data
- Submit data at least once per quarter, no later than 60 days after the end of the quarter

Healthcare Facility Administrators can:

- Upload and update facility information (denominators and injury/illness data)
- Access data submission tools
- Add Facility Administrators (up to five) and Report Users (unlimited) for the facility
- Create and view reports for the facility
- Modify roles or delete users within the facility

Healthcare System Administrators will have all the permissions of a Facility Administrator for each facility within the system and can:

- Add System Administrators (up to five) and System Report Users (unlimited)
- Create and view reports for all individual facilities within the system
- Create and view system aggregate reports
- Add or remove facilities within their healthcare system
- Modify roles or delete users within the system

**Report User Role:**

Healthcare Facility Report Users can:

- Create and view reports for only their facility

Healthcare Facility Report Users cannot:

- Upload or edit information (denominators and injury/illness data) about the facility
- Add, modify or delete users

Healthcare System Report Users can:

- Create and view reports for all facilities within the system
- Create and view system aggregate reports

Healthcare System Report Users cannot:

- Upload or edit information (denominators and injury/illness data)
- Add, modify, or remove users
- Add or remove facilities

**NIOSH OHSN System Administrators** have access rights to all data and user information within the OHSN system.

**NIOSH OHSN Report Users** have the rights to:

- Access OHSN aggregate reports without healthcare system or facility identifiers

NIOSH OHSN Report Users cannot:

- Upload data
- Access data submission tools
- Add or remove a healthcare facility or system
- Add or remove a user or edit user information

### **Acknowledgement and Agreement**

I have read and agree to comply with the terms and condition governing the appropriate and allowed use of OHSN as defined by this document, applicable agency policy, and Federal law. The act of acknowledgement and agreement signifies a clear understanding of the OHSN 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 OHSN.