NIOSH Industry and Occupation Computerized Coding System (NIOCCS)

Rules of Behavior

January 2018

Introduction

The NIOSH Industry and Occupation Computerized Coding System (NIOCCS) is a web-based computer system that translates industry and occupation (I/O) text into standardized I/O codes. It is a tool developed by NIOSH, free of charge to users, which will improve coding uniformity and reduce the high cost of manually coding I/O information from vital records, cancer registries, health care records, and other record systems.

Purpose

These 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 NIOCCS. 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

NIOCCS does not collect personally identifiable information (PII). CDC/NIOSH asks users not to include PII in any data files submitted to NIOCCS for coding.

Users are provided access to NIOCCS 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 NIOCCS user support by sending an email to NIOCCS@CDC.gov.

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

Users shall not engage in, encourage, conceal any “hacking” or “cracking,” denial of service, unauthorized tampering, or unauthorized attempted use of (or deliberate disruption of) any computer system within the NIOCCS 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.

Users will access NIOCCS through a NIOCCS user account and password authentication. Each NIOCCS user will have a unique User Name and password for the system.

A user can only have one logged on session at a time. If a user logs in on one computer then tries to log on again at another workstation without logging out of the previous session, they will be given a choice of canceling the previous session or not continuing with the new log on. This business rule was made to protect a user’s data from conflicting access to the same data files which may cause the data to become corrupt.

Each user is responsible for protecting his/her password. Passwords may be shared, ***however users are responsible for <u>all</u> actions performed with their account.*** Users who believe their password has been compromised in any way should inform NIOSH. Users will supply a password that meets the NIOCCS 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.)

NIOCCS will provide a randomly generated password to the user via email when a user account is first set up or when a ‘Forgot Password’ request is made. Users <u>must</u> change the NIOCCS generated password at next logon.

NIOCCS 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.

NIOCCS System Administrators have access rights to all data and user information within the NIOCCS system.

NIOCCS System Administrators will not share or allow access to data submitted by users to other any person or entity.

NIOCCS System Administrators may review user’s computer assisted coded data periodically to analyze the data for possible inclusion into the NIOCCS knowledge base to improve overall efficiency and accuracy of coding. Once analyzed, NIOSH will delete user files from the CDC server if the file has expired or was removed by the user. A record of all file activity by the user is recorded in the system and can be viewed by the user at any time.