NGSConnex Rules of Behavior

Overview

In this rules of behavior document, the user will learn about the security measures of the NGSConnex application.

Objectives

At the end of this rules of behavior overview the user will be able to:

- Identify the appropriate security measures to follow.
- Identify the Rules of Behavior (ROB).
- Identify the appropriate actions to take to maintain the Centers for Medicare & Medicaid Services (CMS) data integrity.

The rules of behavior covers the following sections:

1. Security
2. Rules of Behavior/Compliance
3. Security Do's and Don'ts
4. Passwords
5. User Account Password Reset
6. Communication

1. Security

Overview

In this section, the user will learn about the security of NGSConnex.

Security Guidelines

Listed below are the minimum requirements presented to all users of NGSConnex before access is granted.

Users serving the role as Local Security Officers (LSOs) must also review the laws and regulations, which govern the actions of NGSConnex users, specifically, the Federal Sentencing Guidelines and Privacy Act of 1974 need to be covered in detail.

The process of reporting a suspected security issue and whom to contact in that case is covered as well. This lets each user know what to do should there be a need to report a potential security issue to assure it is addressed in a proper manner.

Federal Sentencing Guidelines

The Federal Sentencing Guidelines were enacted in the federal government in 1991 as part of the Sentencing Reform Act of 1984.

The Sentencing Reform Act's basic objective was to enhance the ability of the criminal justice system to combat crime through an effective, fair sentencing system.

The Federal Sentencing Guidelines prompted all types of organizations including corporations, partnerships, unions, not-for-profit organizations and trusts to apply fraud and detection measures.

One significant aspect of the Guidelines is that each organization is responsible for the wrongful acts of its employees. The theory is that each organization shares a degree of liability if an employee acts in an unlawful manner, even if the organization did not know of or approve of their actions.

Important factors upon which organizations will be judged by the federal government include:

1. The absence of proper controls.
2. Knowing participation by high level management.
3. Previous violations.
4. Lack of anti-fraud procedures.
5. The absence of ethics training.

Upon conviction, an individual can be sentenced to prison and an organization can be penalized with significant fines.

The Guidelines also establish mitigating circumstances for those organizations that have anti-fraud and specialized internal control programs.

Privacy Act of 1974

The Privacy Act of 1974 provides individuals with a means of access to their system of records that agencies maintain. It permits only an 'individual' to seek access to only his own 'records' and only if that records is maintained by the agency within a 'system of records'.

2. Rules of Behavior/Compliance

Overview

This section explains ROBs for utilizing NGSConnex. Adhering to these requirements is the responsibility of the users accessing NGSConnex. Each user is subject to the same set of requirements, and therefore, has similar ROBs.

Establishing a Set of Rules

A basic set of ROBs follows and serves as minimum requirements for users utilizing NGSConnex. Users are encouraged to implement additional ROBs as long as the rules exceed the ones outlined in this section.

Establishing a Set of Rules for NGSConnex Users

NGSConnex users must follow all rules to protect private information from those who have not been properly identified as having a right to this information.

- Information displayed within NGSConnex is to be discussed only with those individuals within the provider organization who have a need to know.
- Physical workstations should also provide security to keep information private, such as securing the workstation when not at the desk, requiring a User ID and password or token to logon to the workstation.
- NGSConnex has been created to facilitate single requests and does not support automated or scripted lookups.
- The MBI portal look-up tool that is in NGSConnex is to be used only when a Medicare patient doesn't or can't give you his/her Medicare Beneficiary Identifier (MBI). The patient's first name, last name, date of birth and social security number are required to get a unique match. The MBI is confidential so you'll have to protect it as Personally Identifiable Information and use it only for Medicare-related business. You are prohibited from using a computer program to bypass our CAPTCHA security check.
- If a user enters a wrong answer to his or her challenge question three times, their account will be
  – suspended.
- If a user enters their password incorrectly three times, the user will be locked out of his or her account for three hours.
- If an NGSConnex account has not been used within the last 30 days, the account will be disabled. Once an account has been disabled, the user will be required to request a security code to reactivate the account.
- Users are not permitted to access NGSConnex outside of the United States (U.S) and its territories: American Samoa, Guam, Northern Mariana Islands, Puerto Rico and the U.S. Virgin Islands.

NGS reserves the right to deny access and/or disable a user's account without notice when access attempts originate outside the United States or its territories.

Establishing a Set of Rules for LSO Users

In addition to the previous rules for NGSConnex users, LSO users who have the ability to approve, edit or decline access to other users within their organization(s) must follow additional rules.

- LSOs must immediately remove access from users when they leave the organization or no longer have a need to know the information within the application. LSOs should also review and edit system access to ensure that users have the minimum necessary access to information within NGSConnex.
- LSOs are responsible for approving access to users requesting data access to a specific provider account within their organization. Once users have successfully registered for a provider account, the LSO should carefully review the users' requests to ensure they are granted only the access they need.
- LSOs are required to review all user accounts within their organization to ensure that each user has the appropriate access each year; every 365 days.

Penalties for Violating the ROBs

Any user/LSO who violates the ROB is subject to having their user/LSO account revoked.

Individual Accountability

Individuals are responsible for their own actions. Each individual must know and follow all ROBs when utilizing NGSConnex.

LSOs are responsible for ensuring users within their organization are aware of ROBs they are to follow, the rules that apply to them, and the consequences for noncompliance with these rules and procedures.

ROBs and System Access

Each organization/practice is responsible for informing their associates about NGSConnex training materials, ROBs and ensuring they are familiar with them before granting access to NGSConnex.

3. Security Do's and Don'ts

Overview

This section explains what a user should and should not do when performing tasks within NGSConnex that relate to security. In this section the following items will be covered:

- User IDs
- Securing your workstation

User IDs

The guidelines listed below must be followed when using NGSConnex User IDs:

- User IDs, passwords, or other identity credentials should not be shared with other users.
- It is the user's responsibility to remember their User ID.

Workstation Security

Associates should lock their computer or exit the NGSConnex application when they leave their workstation.

4. Passwords

Overview

All users have the capability to change their passwords.

Resetting passwords when an account has been suspended is the responsibility of the LSO.

Passwords

The guidelines listed below must be followed when using NGSConnex passwords:

- Do not keep a written copy of the password at the workstation.
- Do not share the password with anyone.
- If the user is accessing the application and incorrectly types the password three consecutive times, the system will lock the user's account. If the user has forgotten his or her password, he or she should utilize the "Change/Forgot my Password" link to change their password.
- If a user enters incorrect answer to his or her challenge question three times, the account will be suspended.
- Passwords should not be easy to guess.

Password Requirements

The following requirements must be met to change or set up a password.

Password must be between 8 and 30 characters in length and contain 3 of 4 requirements:

1. at least 1 alphabetic character
2. at least 1 numeric character
3. at least 1 special character
4. at least 1 uppercase character

   Examples of **valid** passwords are Cms07Cms or o8T#c3nk$.
   Examples of **invalid** passwords are CMS4 or JANEYDOE.

Details on the steps to follow when changing a password are included in the NGSConnex Training Materials.

5. User Account Password Reset

Overview
User Account Password Reset when an account has been suspended is the responsibility of the LSO and will be done by resetting user passwords.

Purpose
The purpose of resetting user account passwords is to allow users to gain access into NGSConnex once they have suspended their user accounts.

Suspending an account in NGSConnex occurs when a user has entered the answer to their challenge question in the application three times without success. NGSConnex suspends the user's account. The user must request a security code to reset the password to gain access into the application.

User Actions for Password Resets
- Login to NGSConnex and follow the prompts to change the password.
- The first screen that appears in NGSConnex is the 'User Login' screen.
  - The user will enter his or her User ID and password. Upon clicking the ENTER button, the user will be prompted to change the password before proceeding to access NGSConnex.
- Follow the prompts to create a new password.
- The new password must meet the requirements for NGSConnex passwords.

6. Communication

Overview
In this section, the user will learn about communication regarding NGSConnex accounts.

Establishing
NGS may need to provide the user with certain communications, such as Communication service announcements and administrative messages. These communications are considered part of the Services and the user's account, and the user may not be able to opt-out from receiving them.