Reducing Threats and Risks

Privacy, Security, and Fraud: Part 3 of 4

BeWell
New Mexico's Health Insurance Marketplace

Introduction

Previously, the training has covered PII and assister responsibility to report privacy incidents and breaches. This section will discuss strategies for reducing risk using information security individually and as an organization.

BeWell New Mexico's Health Insurance Marketplace

Main Topics

- Information Security Basics
- Information Security Threats
- Organizational Controls and Security
- Promoting Information Security

Information Security Basics

BeWell New Mexico's Health Insurance Marketplace

- Information security refers to the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.
- Information security promotes confidentiality, integrity, and availability of sensitive consumer information.

Information Security Basics (Continued)

- Information security is achieved through implementing technical, managerial, and operational measures designed to protect the confidentiality, integrity, and availability of information.
- In today's work environment, many information systems are electronic; however, both BeWell and the Centers for Medicare and Medicaid Services (CMS) have a media-neutral policy toward information. This means that any data must be protected, whether it is in electronic, paper, or oral format.

Information Security Threats

It is essential that any computers assisters use are protected from harmful computer programs, applications, and malicious software (more commonly known as “malware”). It is an assister’s responsibility to ensure that any office computers used by consumers to access the BeWell application and portals are regularly updated with the latest security software to protect against cyber-related security threats.

Information Security Threats (Continued)

- Assisters may occasionally help consumers using public computers (such as those in libraries).
  - Never save private files to a public computer to upload to an application; it could lead to PII being mistakenly disclosed.
- Email and corrupted websites may deliver malware that infect computers used to access the BeWell applications.
  - Public computers, such as those accessed in a library, may be susceptible to malware and viruses.

Organizational Controls

- Assisters should apply certain controls to protect information within the BeWell eligibility and enrollment (application) system. Controls are policies, procedures, and practices designed to manage risk and protect IT assets.
- Examples of controls include:
  - Security awareness and training programs
  - Physical security like guards, badges, and fences
  - Restricting access to systems that contain sensitive information
- Assisters are required to monitor, periodically assess, and update their security controls and related system risks to maintain continued effectiveness of those controls.

Organizational Controls (Continued)

- Strong passwords are critical to protecting information systems that house PII. Best practices include:
  - Using at least 8 characters, including numbers, upper- and lower-case letters, and special characters;
  - Changing passwords often, and immediately if they may have been compromised;
  - Never sharing passwords;
  - Using a different password for each system or application;
  - Not using a word that can easily be found in a dictionary;
  - Disabling web browsers from remembering passwords; and
  - Using passwords that are not generic or easily obtained (e.g., don't use birthdates or family member names).

Organizational Security

- Access Controls
  - Users should be assigned a unique “User ID” for log-in purposes.
  - Under no circumstances should users log in under a coworker's online account or share their access with anyone, even another authorized user.
  - Access js “role-based.” Users should only have access to a system(s) with PII that they need to use to perform their job. It is limited to the minimum information needed to do their job.
  - When finished working for the day or between meetings with consumers, users should clear their cache and exit out of their internet browser.
    - This disconnects users from the internet and will also help ensure that one consumer’s information is not inadvertently transposed into another consumer’s application.

Protecting Information Security: Individual Protection

- In addition to IT-driven protection, individuals within an organization can take steps to promote information security. They can be "human firewalls" by:
  - Paying attention to details such as when websites connect with HTTP instead of the more secure HTTPS in the address bar;
  - Noticing when someone asks for too much PII and not giving it away unless necessary;
  - Being careful not to hit "Reply All" in an email unless appropriate; and
  - Knowing how to keep information secure.

Promoting Information Security: Social Engineering Scams

BeWell New Mexico's Health Insurance Marketplace

- To avoid social engineering scams, assisters should:
  - Never give anyone their password.
  - Not respond to someone claiming to be a help desk worker asking to confirm their user ID and password.
  - Be aware of links they receive in documents, emails, and chats from unknown sources.
  - Examine messages before clicking on links or responding to them.
  - Not click on or download any link or attachment from an unknown or unexpected email source.
  - Throw it out or call to verify when in doubt.

Promoting Information Security: Physical Security

- Physical security measures include disaster controls, physical access controls, and device and media controls. Examples may include:
  - Ensuring no unauthorized physical access to an unattended device.
  - Configuring devices to “lock” or “auto log-off,” and requiring a user to re-authenticate if left unattended.
  - Not leaving sensitive information on your desk, remote printers, or copiers. Lock doors, windows, etc. when stepping away.
  - Keeping workstations and devices protected from liquids or other harmful substances.

Promoting Information Security: Email Security

- Email security requires various techniques for keeping sensitive information in email communication and accounts secure against unauthorized access, loss or compromise. Email is also a popular medium for the spread of malware, spam, and phishing attacks. Assisters should take the following precautions to maintain information security when emailing:
    - Confirm email addresses before sending;
    - Send emails only to those who need the information;
    - Attach a confidentiality clause to all emails; and
    - Encrypt emails containing PII or other confidential or sensitive consumer data.

Promoting Information Security: Encryption

- Encryption
  - Encryption is the process of converting text or data to prevent it from being read or accessed by individuals who are not authorized.
  - Email encryption is a security control that protects the content from being read by entities other than the intended recipient(s).
  - Email encryption can rely on public-key cryptography, in which users can each publish a public key that others can use to encrypt messages to them while keeping secret a private key they can use to decrypt such messages or to digitally encrypt and sign messages they send.
  - **Note**: Assisters should reach out to their IT person or manager for more information on encrypting emails, when necessary.

Promoting Information Security Instant Messaging

- Instant Messaging
  - IM and Instant Relay Chat (IRC) or chat rooms create ways to communicate or chat in “real-time” over the Internet.
  - Like email, exercise extreme caution should be used when using IM.
  - Maintain up-to-date virus protection and firewalls, since IM may leave networks vulnerable to viruses and spam, and open to attackers/hackers.
  - Be aware that this area of the Internet is not private.
  - Discourage consumers from sending sensitive PII or PHI via email, unless encrypted, or via chat.

Promoting Information Security: Faxing Documents

BeWell New Mexico's Health Insurance Marketplace

- Assisters should use the following precautions whether they are faxing a physical document or an electronic file:
  - Confirm the recipient's number before sending.
  - Attach their confidentiality clause on the cover page.
  - Maintain control of the paper documents immediately after the fax has been sent.
  - Confirm the receipt of the fax if highly confidential.
  - Faxing of Federal Tax Information (FTI) is prohibited.

Promoting Information Security: Wireless/Remote Work

- Assisters should take the following precautions to minimize risk when using wireless devices or working remotely:
  - Do not enable the wireless port that exposes the device, unless it has been secured.
  - Use a Virtual Private Network (VPN) if making a wireless connection, adhere to user/device authentication before transmitting PII wirelessly, encrypt data during transmission, and maintain an audit trail.
  - Try not to work with sensitive information in public places.
    - **Note**: If assisters must work with sensitive information in public places, they should always use a VPN. They should also use a screen shield so the information displayed is not in plain view.

Promoting Information Security: Back-up Systems

BeWell New Mexico's Health Insurance Marketplace

- System back-ups are created to assure integrity and reliability. Technology Departments can provide information about an organization's back-up procedures. Assisters should:
  - Follow IT support group procedures if there is need to temporarily store data on local drives or laptops.
  - Back up original data files with PII and other essential data and software programs frequently based on data criticality, either daily, weekly, or monthly.
  - Store back-up files at a geographically separate and secure location.
  - Prepare for disasters by testing the ability to restore data from back-up tapes/disks.
  - Consider encrypting back-up disks for further protection of confidential information; refer to internal organizational policies and experts for further information.
  - Permanent copies of PII should not be stored for archival purposes on portable equipment such as laptop computers and memory sticks.

Promoting Information Security: Destroying Data

- Electronic Data
  - Destroy electronic PII data which is no longer needed by “cleaning” hard-drives, CDs, flash/thumb drives, or back-up recordings before recycling or re-using electronic media.
  - Have an IT professional overwrite, degauss, or destroy your digital media before discarding via magnets or special software tools.
- Shredding
  - When finished with paper documents, shred them, following the guidelines in IRS Publication 1075.
  - Use a cross-cut shredder, which makes reconstructing documents very difficult.

Key Points

- Information security refers to the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.
- Assisters must make sure that any computers they use to store consumer PII are protected from harmful computer programs, applications, and malware and are regularly updated with the latest security software to protect against any cyber-related security threats.
- Steps assisters can take to promote information security include changing their passwords often, using different passwords for each system or application, and not sharing their password with others.


BeWell
New Mexico's
Health Insurance
Marketplace