Handling Privacy and Security Incidents and Breaches

Privacy, Security, and Fraud: Part 2 of 4

BeWell
New Mexico's Health Insurance Marketplace

Introduction

Protecting consumers' personally identifiable information (PII) is one of the most important responsibilities of an assister (a general term used for agents, brokers, and enrollment counselors (ECs)). If an incident occurs in which that information is compromised, it is important for assisters to be able to recognize it and know what steps to take.

Main Topics

- Terms and Examples
- Compromised PII
- Reporting a Breach
- Consequences of Not Protecting PII

Terms and Examples (1 of 3)

- Security Incidents vs. Privacy Incidents
  - A security incident is a potential threat to the confidentiality, integrity, or availability of personally identifiable information (PII). It is the act (or attempt) of violating an explicit or implied security policy, which includes attempted or successful unauthorized access, use, disclosure, modification, or destruction of data or interference with system operations in an information system.
  - A privacy incident is a security incident that involves PII where individuals other than authorized users have access to PII.

Terms and Examples (2 of 3)

BeWell New Mexico's Health Insurance Marketplace

- Examples of Privacy Incidents include:
  - Losing encrypted or unencrypted electronic devices that contain PII (e.g., laptops, cell phones, disks, thumb drives, flash drives, and CDs).
  - Losing hard copy documents containing PII.
  - Sharing paper or electronic documents containing PII with individuals who are not authorized to access the information.
  - Accessing paper or electronic documents containing PII without authorization or for reasons not related to job performance.

Terms and Examples (3 of 3)

BeWell New Mexico's Health Insurance Marketplace

- Examples of Privacy Incidents:
  - Emailing or faxing documents containing PII to inappropriate recipients, whether intentional or unintentional
  - Posting PII to a public-facing website, whether intentional or unintentional
  - Mailing hard copy documents containing PII to an incorrect address, whether intentional or unintentional
  - Leaving documents containing PII exposed in an area where individuals without approved access could read, copy, or move for future use

Compromised PII

- A breach is a privacy incident that poses a risk of harm to applicable individuals.
- The determination of whether a privacy incident involving an application submitted to BeWell rises to the level of a breach is made by the BeWell IT Security and Compliance Manager.
- Assisters should have written procedures in place for addressing privacy and security incidents.

Compromised PII (Continued)

If an assister learns of a situation in which a consumer's PII has been compromised, including unauthorized persons seeing or possessing the information or losing the records, the incident should be reported to the BeWell IT Security and Compliance Manager at PrivacyOfficer@nmhix.com within one hour of discovery.

Reporting a Breach

- What types of issues should be reported?
  - Lost, stolen, or misplaced records or computers
  - Unauthorized personnel or other third parties seeing or possessing PII
  - Incidents with the potential to compromise consumer information

Reporting a Breach (Continued)

- Assisters must implement and comply with breach and incident handling procedures that detail the identification, response, recovery, and follow-up of incidents and breaches.
- These procedures must be in writing, address how to identify incidents, and identify any designated personnel (i.e., a privacy official or officer) responsible for managing incidents or breaches and reporting them to the BeWell IT Security and Compliance Manager.
- Procedures must require reporting of any incident or breach of PII to the BeWell IT Security and Compliance Manager at PrivacyOfficer@nmhix.com within one hour of discovery.

Consequences of Not Protecting PII

- If an assister fails to protect consumers' information and/or purposefully disclose their PII for an unauthorized purpose, any of the following might occur:
  - Consumers' identities may be stolen;
  - The assister may lose consumers' trust;
  - The assister will be out of compliance with the standards of BeWell and CMS;
  - The assister may lose their authority from BeWell to assist consumers enrolling in health coverage through BeWell; or
  - The assister may be at risk for a civil monetary penalty (CMP) by the federal government and/or criminal charges.

Consequences of Not Protecting PII (Continued)

- If an assister fails to protect consumers' information and/or purposefully disclose their PII for an unauthorized purpose, any of the following might occur:
  - Civil Penalties
    - Any person who knowingly and willfully uses or discloses information in violation of section 1411(g) of the ACA will be subject to a civil penalty of not more than $25,000 per person or entity, per use or disclosure, in addition to other penalties that may be prescribed by law.
  - Criminal Penalties
    - Criminal Penalties can include a misdemeanor criminal charge and $5,000 fine.

Key Points

- A privacy incident occurs any time people have access or potential access to PII when they're not authorized to, or when they use PII for an unauthorized purpose. A privacy incident can arise from any number of causes.
- A breach is a privacy incident that poses a reasonable risk of harm to the applicable individuals. Any suspected breach should be reported immediately.
- Assisters should have written procedures in place for addressing privacy and security incidents.
- Assisters must report all PII incidents and breaches to the BeWell IT Security and Compliance Manager at PrivacyOfficer@nmhix.com within one hour of discovery.


BeWell
New Mexico's
Health Insurance
Marketplace