Breaches of Unsecured Protected Health Information

Overview

The Health Information Technology for Economic and Clinical Health Act (HITECH) extends the range of privacy and security protections that are already exist under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA provides federal protections of personal health information held by covered entities and gives the individuals varies rights with regards to their health information. The HITECH Act requires Covered Entities[1] and Business Associates[2] under HIPAA to notify the Secretary of Health and Human Services (HHS) of any security breaches of protected health information (PHI).[3] HHS defines a breach as an impermissible use or disclosure of PHI under the HIPAA Privacy Rule that compromises the security of privacy of the PHI such that the use or disclosure poses a significant risk of financial, reputation or other harm to the affected individual.[4] Covered Entities and Business Associates can submit a breach report electronically to the Office of Civil Rights (OCR), within the HHS.

Breach Notification Requirements

The purpose of the breach notification requirements is to encourage covered entities and business associates to secure PHI to the extent possible to avoid unauthorized uses and disclosures of the information. The following outlines the categories of breach notices:

- Individual Notice – Covered entities must provide notification in written form, by first-class mail, or alternatively, by e-mail if individual has agreed to receive such notices electronically no later than 60 calendar days following the discovery

- Media Notice – For breaches involving more than 500 residents of a State or jurisdiction a covered entity must provide notice to media outlets serving the State or jurisdiction no later than 60 calendar days following the discovery.

- Notice to Covered Entity – For breaches involving any number of individuals, business Associates must notify the covered entity of a breach without delay and no longer than 60 days from the discovery of a breach.

- Notice to Secretary – Notification of a breach that affects 500 or more individuals requires notification to the Secretary of HHS without delay no later than 60 days following the breach. For breaches that affect fewer than 500 individuals, the covered entity may notify the Secretary on an annual basis and submit a report no later than 60 days after the end of the calendar year in which the breaches occurred.

Security Measures to Protect PHI

In addition to providing the required notifications, covered entities reported, as part of their reporting to HHS, taking one or more of the following step to mitigate the potential consequences of breaches only affecting 500 or more individuals and prevent future breaches:

- Revise policies and procedures
- Improve physical security
- Train or retrain workforce members
- Provide free credit monitoring to customers
- Adopt encryption technologies
- Impose sanctions
- Change passwords
- Perform a new risk assessment
- Revise business associate contracts

Summary of Annual Breach Report

HHS's *Annual Report to Congress on Breaches of Unsecured Protected Health Information* outlines the types and numbers of breaches that occurred between September 23, 2009 (the date the breach notification requirements became effective), and December 31, 2010. The report provides the following information on breaches involving 500 or more individuals:

---

[1] Covered entity is defined as a facility, health plan, or health care clearinghouse that transmit medical information in electronic form
[2] A person or entity using (PHI) to perform a function or activity on behalf of a covered entity but who is not part of the aforementioned workforce
[3] Enacted as part of the American Recovery and Reinvestment Act of 2009
[4] Definition of breach and exceptions as defined in HIPAA is available at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html

September 2009 – December 2009

From September through December 2009, covered entities notified approximately 2.4 million individuals that were affected by breaches. HHS received 45 breach notifications that affected 500 or more individuals. The general causes of these incidents are listed in Figure 1.

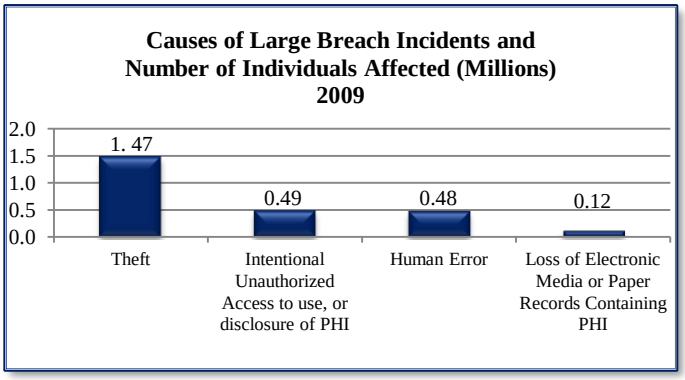

Figure 1

Theft accounted for the largest number of breaches at about 27 incidents (60%) that affected at least 1.4 million individuals. These incidents occurred both on- and off–site and involved the following.

- On-site incidents of theft
  - 17 electronic devices
  - 8 desktop computers
  - 4 laptops
  - 6 hard drives or other equipment
  - 1 portable electronic devices
- Off-site incidents of theft
  - 4 laptops
  - 3 portable electronic devices
  - 2 hard drives and other medical equipment
  - 1 paper records

About four of the 27 incidents impacted the largest numbers of individuals; the details are provided in Figure 2.

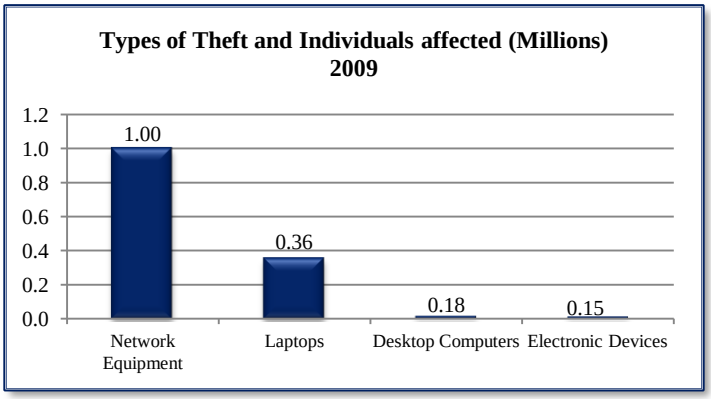

Figure 2

January 2010 – December 2010

From January through December 2010, covered entities notified approximately 5.4 million individuals who were affected by breaches. The HHS received 207 breach notifications that affected 500 or more individuals. The major causes of incidents and number of individuals affected are provided in Figure 3.

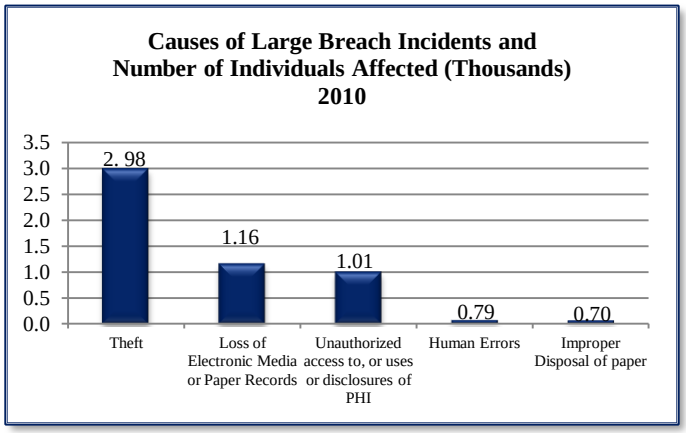

Figure 3

As in 2009, theft accounted for the largest number of breaches at 99 incidents (48%) that affected approximately 2.9 million individuals.

Small Breaches (under 500)

From September through December 2009, approximately 5,521 reports of small breaches were reported to the HHS, or breaches affected around 12,000 individuals. HHS received more than 25,000 reports of small breaches during 2010, which affected more than 50,000 individuals. The majority of these breaches for both years involved misdirected communications and only affected one individual in each case.

Covered entities are taking corrective actions to provide relief and mitigation to individuals and to secure their data and prevent breaches from occurring in the future. The OCR continues reviewing and responding to breach notification reports and establishing investigations into all breaches involving 500 or more individuals.

For the full report to Congress on the Breach Notification Program: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachrept.pdf or visit HHS for more information on Notification of Breaches at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html