Annual Report to Congress on Breaches of Unsecured Protected Health Information

For Calendar Years 2009 and 2010

As Required by the
Health Information Technology for Economic and Clinical Health (HITECH) Act,
Public Law 111-5, Section 13402

Submitted to the
Senate Committee on Finance,
Senate Committee on Health, Education, Labor, and Pensions,
House Committee on Ways and Means, and
House Committee on Energy and Commerce

U.S. Department of Health and Human Services
Office for Civil Rights

Introduction

Section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5), requires covered entities and business associates under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to provide notification of breaches of unsecured protected health information.

Section 13402(i) of the HITECH Act requires the Secretary of Health and Human Services ("the Secretary") to prepare and submit to the Senate Committee on Finance, the Senate Committee on Health, Education, Labor, and Pensions, the House Committee on Ways and Means, and the House Committee on Energy and Commerce, an annual report containing the number and nature of breaches reported to the Secretary, and the actions taken in response to those breaches. The following report was prepared to fulfill this statutory requirement. It provides an overview of the breach notification requirements, as well as a discussion of the reports the Secretary received as a result of these new requirements of the breaches that occurred in calendar years 2009 and 2010.

Background

Section 13402 of the HITECH Act requires HIPAA covered entities to notify affected individuals, the Secretary, and in some cases the media following the discovery of a breach of unsecured protected health information. Business associates are also required to notify covered entities following the discovery of a breach.

Section 13402(h) of the HITECH Act defines "unsecured protected health information" as "protected health information that is not secured through the use of a technology or methodology specified by the Secretary" in guidance, and requires the Secretary to specify in the guidance the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals.

The U.S. Department of Health & Human Services ("the Department") first issued the guidance on April 27, 2009 (74 FR 19006), with a request for public comment. On August 24, 2009, the Department issued its Breach Notification for Unsecured Protected Health Information Interim Final Rule (IFR) (74 FR 42740) that implemented the breach notification requirements of section 13402 of the HITECH Act with respect to HIPAA covered entities and business associates. The IFR included an update to the guidance and identified encryption and destruction as the technologies and methodologies for rendering protected health information unusable, unreadable, or indecipherable to unauthorized individuals (74 FR 42741).

Covered entities and business associates that render protected health information unusable, unreadable, or indecipherable in accordance with the guidance are relieved from providing notifications following a breach of such information. Thus, the purpose of the breach notification requirements and guidance is to encourage covered entities and business associates to secure protected health information to the extent possible to avoid unauthorized uses and disclosures of the information. Covered entities that do not secure protected health information

using the technologies and methodologies identified in the guidance must inform the affected individuals, the Secretary, and in some cases, the media, of breaches to ensure appropriate steps are taken to mitigate any consequences of the breach and to avoid similar incidents in the future, as well as to promote public transparency regarding such incidents.

Definition of Breach

Consistent with the definition of breach in section 13400(1)(A) of the HITECH Act, the Department defines breach at 45 CFR § 164.402 as the acquisition, access, use, or disclosure of protected health information in a manner not permitted by the HIPAA Privacy Rule[1] which compromises the security or privacy of the protected health information.

Section 13400(1)(B) of the HITECH Act provides several exceptions to the definition of breach. These exceptions generally are mirrored in 45 CFR § 164.402. Section 164.402 excludes as a breach: (1) any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate, if made in good faith and within the scope of authority, and if it does not result in further impermissible use or disclosure; (2) any inadvertent disclosure of protected health information by a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information is not further impermissibly used or disclosed; and (3) a disclosure of protected health information where a covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made would not reasonably have been able to retain the information.

Breach Notification Requirements

Following the discovery of a breach of unsecured protected health information, covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain cases, to the media. In the case of a breach of unsecured protected health information at or by a business associate of a covered entity, the business associate must notify the covered entity of the breach. These breach notification requirements for covered entities and business associates are set forth at 45 CFR §§ 164.404 – 164.410.

- **Individual Notice**

  Covered entities must notify affected individuals of a breach of unsecured protected health information without unreasonable delay and in no case later than 60 calendar days following discovery of the breach. Covered entities must provide written notification by first-class mail at the last known address of the individual or, if the individual agrees to electronic notice, by e-mail. If the covered entity knows the individual is deceased and has the address of the next

[1] The Privacy Rule strikes a balance that protects the privacy of the health information of individuals while permitting important uses and disclosures of the information, such as for treatment of an individual and payment for health care, for certain public health purposes, in emergency situations, and to the friends and family involved in the care of an individual.

of kin or personal representative of the individual, then the covered entity must provide written notification to the next of kin or personal representative. Individual notification may be provided in one or more mailings as information becomes available regarding the breach.

If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute notice in the form of either a conspicuous posting for 90 days on the home page of its Web site or conspicuous notice in major print or broadcast media in geographic areas where the affected individuals likely reside, and include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's information may be included in the breach. In cases in which the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written notice, telephone, or other means.

Whatever the method of delivery, the notification must include, to the extent possible: (1) a brief description of what happened, including the date of the breach and the date of discovery of the breach, if known; (2) a description of the types of unsecured protected health information involved in the breach; (3) any steps individuals should take to protect themselves from potential harm resulting from the breach; (4) a brief description of what the covered entity is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and (5) contact information for individuals to ask questions or learn additional information. 45 CFR § 164.404.

- **Media Notice**

For breaches involving more than 500 residents of a State or jurisdiction, a covered entity must notify prominent media outlets serving the State or jurisdiction. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach, as well as include the same information as that required for the individual notice. 45 CFR § 164.406.

- **Notice to the Secretary**

In addition to notifying affected individuals and the media (where appropriate), a covered entity must notify the Secretary of breaches of unsecured protected health information. If a breach involves 500 or more individuals, a covered entity must notify the Secretary at the same time the affected individuals are notified of the breach. A covered entity must also notify the Secretary of breaches involving fewer than 500 individuals, but it may submit reports of such breaches on an annual basis. Reports of breaches involving fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches occurred. 45 CFR § 164.408. Covered entities must notify the Secretary by filling out and electronically submitting a breach report form on the OCR web site at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.

- **Notification by a Business Associate**

If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify the covered entity following the discovery of the breach so that the covered entity can notify the affected individuals, the Secretary, and the media, if appropriate, of the breach (or delegate the notification responsibilities to the business associate). A business associate must provide notice to the covered entity without unreasonable delay and no later than 60 calendar days from the discovery of the breach. To the extent possible, the business associate must identify each individual affected by the breach, as well as include any other available information that the covered entity is required to include in its notification to individuals. 45 CFR § 164.410.

Summary of Breach Reports

This report describes 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 numbers of affected individuals are approximate because some covered entities reported uncertainty about the number of records affected by a breach. For reports of breaches involving 500 or more individuals, we have excluded those incidents that occurred before the effective date of the IFR. In all other instances, if a covered entity chose to provide notification of the breach, we have included the incident in the counted breaches, even if an exception to the definition of "breach" may have applied based on the circumstances of the incident.

The following analysis provides a snapshot of breaches that occurred during the specified time period based on the breach reports submitted to the Secretary. The report also describes actions that have been taken by covered entities in response to the reported breaches.

Breaches Involving 500 or More Individuals

Notification to the Secretary of breaches involving 500 or more individuals must occur contemporaneously with notice to affected individuals. OCR received 45 reports of such breaches occurring during the approximately three-month reporting period in calendar year 2009 (September 23, 2009, to December 31, 2009) and 207 reports in calendar year 2010, the first full calendar year for reporting**.** In 2009, covered entities notified approximately 2.4 million individuals who were affected by these large breaches. In 2010, covered entities notified approximately 5.4 million individuals affected by these large breaches.

Common Causes of Large Breaches in 2009

The breach reports submitted to the Secretary in 2009 described four general causes of incidents: (1) theft; (2) intentional unauthorized access to, use, or disclosure of protected health information; (3) human error; and (4) loss of electronic media or paper records containing protected health information.

Theft was reported as the most common cause of large breach incidents. Among the 45 breaches that affected 500 or more individuals, 27 incidents involved thefts of paper records or electronic media, affecting approximately 1,468,578 individuals. Intentional unauthorized access to, or uses

or disclosures of, protected health information affected approximately 483,686 individuals. Human or technological errors, or other failures to take adequate care of protected health information, affected approximately 477,209 individuals. Finally, loss of electronic media or paper records affected approximately 11,592 individuals.

Of the 27 incidents involving theft, 17 occurred on the premises of the covered entity or its business associate, with some involving the theft of more than one electronic device. Eight onsite thefts involved stolen desktop computers, four involved stolen laptops, six involved stolen hard drives or other equipment, and one incident involved a stolen portable electronic device. Ten incidents involved theft from an offsite location, usually the vehicle of an employee. These incidents included four thefts of laptops, three thefts of portable electronic devices, two thefts of hard drives and other medical equipment, and one theft of paper records.

The four discrete incidents of theft that reportedly affected the largest numbers of individuals involved the theft of network equipment (998,422 individuals affected), laptops stolen from a covered entity's facility (359,000 individuals affected), a desktop computer stolen from an office shared by several covered providers (18,377 individuals affected), and the theft of a portable electronic device from an offsite location (15,500 individuals affected).

The second category of large breaches involved four incidents of intentional, unauthorized access to protected health information. In one case, a "phishing" scam led a covered entity's employee to share login information for an email inbox, potentially exposing the protected health information of 610 individuals. Another covered entity reported discovering that two employees, who had access to the protected health information of 1,076 individuals, had misused patient credit card information. A third incident involved a third party hacking into a covered entity's network, gaining access to the protected health information of 2,000 individuals. Finally, a fourth incident involved a third party exploiting a security vulnerability to gain access to the protected health information of 480,000 individuals through the covered entity's web portal.

Human or technological error, or other failure to take adequate care of protected health information, was responsible for ten breaches that affected approximately 477,209 individuals. One covered entity reported that it had discovered that hard drives in more than twenty photocopiers it had previously leased, which had since been sold by a wholesaler, might contain the confidential information of up to 344,579 individuals. Other incidents involved: (1) one business associate that printed and mailed letters to 83,000 individuals whose insurance plan identification numbers were printed conspicuously on the outside of the mailing; (2) two covered entities' misdirected mailings to more than 18,000 individuals; and (3) one covered entity's uploading the records of 9,000 individuals to an unsecured website.

Four covered entities reported lost or misplaced protected health information affecting a total of 11,592 individuals. Each incident involved a different form of protected health information: backup tapes (one incident involving 2,562 individuals), a portable electronic device (one incident involving 3,800 individuals), a laptop (one incident involving 3,800 individuals), and paper records (one incident involving 1,430 individuals).

Common Causes of Large Breaches in 2010

The breach reports submitted to the Secretary in 2010 described five general causes of incidents, four of which were also reported in 2009: (1) theft; (2) loss of electronic media or paper records containing protected health information; (3) unauthorized access to, use, or disclosure of protected health information; (4) human error; and (5) improper disposal. In comparison to 2009, in 2010, the number of individuals affected by the loss of electronic media or paper records was greater than those affected by unauthorized access or human error. Moreover, the reports received in 2010 contained incidents involving an additional category, improper disposal of paper records by the covered entity or business associate.

Theft was once again the most common reported cause of large breaches. Among the 207 breaches that affected 500 or more individuals, 99 incidents involved theft of paper records or electronic media, together affecting approximately 2,979,121 individuals. Loss of electronic media or paper records affected approximately 1,156,847 individuals. Unauthorized access to, or uses or disclosures of, protected health information affected approximately 1,006,393 individuals. Human or technological errors, or other failures to take adequate care of protected health information, affected approximately 78,663 individuals. Improper disposal of paper affected approximately 70,279 individuals. In addition to these five categories of breaches, the remaining large breaches were reported with an unknown cause or the covered entity's description demonstrated uncertainty as to the exact cause.

Of the 99 incidents involving theft, the largest reported theft affected approximately 1.9 million individuals. This reported breach involved theft of back-up tapes that contained electronic medical records as they were being transported by a vendor from the covered entity to the vendor's site. Additionally, forty-two of the reported incidents involved the theft of laptops. The majority of the incidents involved thefts of laptops onsite while a few incidents involved offsite theft, such as theft of a laptop from an employee's car. Twenty-one incidents involved theft of desktop computers from onsite locations. Fourteen incidents were reported by covered entities as theft of "portable electronic device/other." These incidents predominately involved stolen smart phones and flash drives. Finally, seven incidents were reported as thefts of more than one device, such as a laptop and a desktop computer or a desktop computer and network drive, and five incidents involved theft of a network server from the covered entity or business associate.

The second category of large breaches involved the loss of electronic media or paper records. The thirty-three reported cases affected more than 1,156,847 individuals. The majority of these cases, twenty-three, were reported as the loss of other portable electronic devices (i.e., not involving laptops). Several of these cases involved the loss of back-up tapes, compact discs, memory cards, flash drives, and smart phones. In one case, a covered entity contracted with a business associate to destroy back-up tapes containing protected health information that was no longer compatible with the hospital's computer system. The business associate hired a third party to destroy the material but later informed the covered entity that several of the tapes were unaccounted for at the time of destruction and as a result, approximately 800,000 individuals were affected. Another case involved the loss of unencrypted back-up tapes containing the protected health information of more than 19,000 individuals. The remaining ten cases reported

by covered entities as a "loss" involved the loss of laptops, paper records, or a network hard drive.

Covered entities reported thirty-one breaches that involved unauthorized access to, or uses or disclosures of, protected health information. The thirty-one breaches affected a total of 1,006,393 individuals. Twelve of the thirty-one unauthorized access cases involved hacking incidents where information from desktop computers or network servers was improperly accessed by others. For example, one hacking incident compromised a network server and as a result, the prescription information of approximately 27,000 individuals was impermissibly displayed. In addition to hacking incidents, several unauthorized access cases involved unauthorized employees accessing protected health information or authorized employees engaging in an unauthorized use of the protected health information. For example, a covered entity reported an incident where an employee emailed unencrypted protected health information to a personal email account and as a result, put the protected health information of more than 2,000 individuals at risk. Yet another incident involved an employee who disclosed the protected health information of thousands of individuals to a third party, without valid authorization, for personal gain. The largest unauthorized access case reported in 2010 involved an employee who was no longer employed by the covered entity but still had access to a password protected website containing individuals' protected health information. As a result, approximately 400,000 individual's protected health information was impermissibly accessed by an unauthorized individual.

Nineteen covered entities reported breaches that occurred because of human or technological error affecting approximately 78,663 individuals. The most common cases consisted of misdirected mailings involving paper records, where individuals received another patient's protected health information because the mailing address was listed incorrectly. Additionally, some breaches were reported as technological incidents involving email and network servers. For example, a number of covered entities reported incidents where an email containing unencrypted protected health information was sent to the wrong recipient or where patients' email addresses should have been included in a blind carbon copy ("BCC") line but were instead visible to the other recipients.

Eleven covered entities reported breaches that occurred because of improper disposal of protected health information and affected a total of approximately 70,279 individuals. All eleven cases involved the improper disposal of protected health information in paper records. The majority of the cases reported mishandling of information on the part of a covered entity's business associate. In one case, a covered entity's business associate, a third party billing service, improperly disposed of two years worth of hospital records containing patients' names, addresses, social security numbers, diagnoses, etc. This breach affected approximately 20,000 individuals. Another covered entity reported an incident in which its business associate, also a billing service, improperly disposed of protected health information in a public area and the records were recovered by a reporter. This incident affected more than 24,000 individuals.

Remedial Action Reported

In addition to providing the required notifications, in 2009 and 2010, covered entities most commonly reported taking one or more of the following steps to mitigate the potential consequences of breaches affecting 500 or more individuals and prevent future breaches:

- Revising policies and procedures;
- Improving physical security by installing new security systems or by relocating equipment or records to a more secure area;
- Training or retraining workforce members who handle protected health information;
- Providing free credit monitoring to customers;
- Adopting encryption technologies;
- Imposing sanctions on workforce members who violated policies and procedures primarily in response to serious employee errors, removing protected health information from the facility against policy, and unauthorized access;
- Changing passwords;
- Performing a new risk assessment; and
- Revising business associate contracts to more explicitly require protection for confidential information.

In both 2009 and 2010, with respect to large breaches involving either paper records or electronic protected health information, revising policies and procedures appeared to be the most common remedial action taken by covered entities. Improving physical security, providing additional training to workforce members, and providing free credit monitoring to impacted individuals were also among the most common steps taken by covered entities after experiencing these large breaches. With respect to large breaches involving the theft or loss of electronic protected health information, of the approximately 131 reports of such breaches in 2009 and 2010, about fifty percent of the reports indicated that encryption technologies were being implemented as a remedial step to avoid future breaches.

Breaches Involving Fewer than 500 Individuals

A covered entity must notify the Secretary of breaches involving fewer than 500 individuals. Reports of breaches involving fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches occurred. For breaches that occurred during 2009, notification to the Secretary was required no later than March 1, 2010. For breaches that occurred during 2010, notification to the Secretary was required no later than March 1, 2011.

HHS received approximately 5,521 reports of smaller breaches that occurred between September 23, 2009, and December 31, 2009. These smaller breaches affected approximately 12,000 individuals. HHS received more than 25,000 reports of smaller breaches that occurred between January 1, 2010, and December 31, 2010. These smaller breaches affected more than 50,000 individuals.

Common Causes and Remedies

The majority of small breach reports in 2009 and 2010 involved misdirected communications and affected just one individual each. Often, a clinical or claims record of one individual was mistakenly mailed or faxed to another individual. In other instances, test results were sent to the wrong patient, files were attached to the wrong patient record, emails were sent to the wrong addresses, and member ID cards were mailed to the wrong individuals.

In response to these incidents, covered entities commonly reported fixing "glitches" in software that incorrectly compiled lists of patient names and contact information, revising policies and procedures, and training or retraining employees who handled protected health information.

Summary and Conclusion

Between September 23, 2009, and December 31, 2009, breaches involving 500 or more individuals made up less than one percent of reports but accounted for more than 99 percent of the more than 2.4 million individuals who were affected by a breach of their protected health information. The largest breaches occurred as a result of theft, error, or a failure to take adequate care of protected health information. The greatest number of reported incidents resulted from human or technological error and involved the protected health information of just one individual.

Between January 1, 2010 and December 31, 2010, breaches involving 500 or more individuals also made up less than one percent of reports, yet accounted for more than 99 percent of the more than 5.4 million individuals who were affected by a breach of their protected health information. The largest breaches in 2010, like 2009, occurred as a result of theft. However, in comparison to 2009, in 2010, the number of individuals affected by the loss of electronic media or paper records containing protected health information was greater than the number of individuals affected by unauthorized access or human error. Furthermore, the reports received in 2010 contained incidents involving an additional category, improper disposal of paper records by

the covered entity or business associate. The greatest number of reported incidents in 2010 once again resulted from small breaches involving human or technological error, and most commonly these incidents involved the protected health information of just one or two individuals.

The breach notification requirements are achieving their twin objectives of increasing public transparency in cases of breach and increasing accountability of covered entities. The reports submitted to the Secretary indicate covered entities and business associates are providing notifications in the event of breaches. Millions of affected individuals are receiving notifications, local media are being notified in the regions where the covered entities operate, and the Secretary is receiving thousands of breach reports. To provide increased public transparency, information about breaches involving 500 or more individuals is available for public view on the OCR website at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html. The breaches are posted in an accessible format that allows users to search and sort the posted breaches by name of covered entity, state, number of individuals affected, date of breach, type of breach, and location of the breached information (e.g., laptop computer). Additionally, the website provides brief summaries of the breach cases that OCR has investigated and closed.

At the same time, more entities are taking remedial action to provide relief and mitigation to individuals and to secure their data and prevent breaches from occurring in the future. In addition, OCR continues to exercise its oversight responsibilities by reviewing and responding to breach notification reports and establishing investigations into all breaches involving 500 or more individuals. To date, of the 252 breaches involving 500 or more individuals occurring in 2009 and 2010, OCR has closed approximately 76 of these cases where, through its investigation, OCR determined that the covered entity properly complied with the breach notification requirements, and that the corrective action taken by the covered entity appropriately addressed the underlying cause of the breach so as to avoid future incidents and mitigated any potential harm to affected individuals. In the remaining cases, OCR continues to investigate the reported incidents and to work with the covered entities to ensure appropriate remedial action is taken to address and prevent future incidents and to mitigate harm to affected individuals, as well as to ensure full compliance with the breach notification requirements.