Annual Report to Congress on Breaches of Unsecured Protected Health Information

For Calendar Years 2011 and 2012

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 (PHI).

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 provides the required information for the breaches reported to the Secretary that occurred in calendar years 2011 and 2012.[1]

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 PHI. Business associates are also required to notify covered entities following the discovery of a breach. Section 13402(h) of the 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 provides that the guidance specify the technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized persons. The guidance issued by the Secretary (last update August 24, 2009, 74 FR 42740) identifies encryption and destruction as the two technologies and methodologies for rendering PHI unusable, unreadable, or indecipherable to unauthorized persons. Covered entities and business associates that encrypt or destroy PHI in accordance with the guidance are not required to provide notifications in the event of a breach of such information because the information is not considered "unsecured."

The U.S. Department of Health & Human Services ("the Department") issued its Breach Notification for Unsecured Protected Health Information Interim Final Rule (74 FR 42740) on August 24, 2009, to implement the breach notification requirements of section 13402 of the HITECH Act with respect to HIPAA covered entities and business associates. On January 25, 2013, the Department published modifications to and made permanent the provisions of the Breach Notification Rule (78 FR 5566).

[1] To provide more robust data than would be available from analyzing a single year, the first Report to Congress covered the period from September 23, 2009 (the date the breach notification requirements became effective), through the end of 2010. Similarly, this Report to Congress covers a 2-year period, allowing the Department to better compare trends and outcomes from one year to the next, in addition to providing cumulative data.

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 PHI in a manner not permitted by the HIPAA Privacy Rule[2] which compromises the security or privacy of the PHI. Under the Breach Notification Rule, an unauthorized acquisition, access, use, or disclosure of PHI (that does not fall into one of the enumerated exceptions discussed below) is presumed to be a breach unless the covered or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment. This risk assessment must address at least the following factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person(s) who used the PHI or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated.

Section 13400(1)(B) of the HITECH Act provides several exceptions to the definition of "breach." These exceptions generally are mirrored in the regulations at 45 CFR § 164.402. Section 164.402 excludes as a breach: (1) any unintentional acquisition, access, or use of PHI 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 PHI by a person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI 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 PHI 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 PHI, covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain cases, the media. In the case of a breach of unsecured PHI 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 PHI without unreasonable delay and in no case later than 60 calendar days following discovery of the

[2] 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.

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 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 PHI 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 PHI. 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 were discovered. 45 CFR § 164.408. Covered entities must notify the Secretary by filling out and electronically submitting a breach report form on the Department web site at

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.

- **Notification by a Business Associate**

If a breach of unsecured PHI occurs at or by a business associate, the business associate must notify the covered entity following the discovery of the breach. 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 (although a covered entity and business associate may negotiate stricter timeframes for the business associate to report a breach to the covered entity). To the extent possible, the business associate must identify each individual affected by the breach, as well as include any other available information that is required to be included in the notification to individuals. While a covered entity ultimately maintains the obligation to notify the affected individuals, the Secretary, and the media (if appropriate) where a breach occurs at or by its business associate, a covered entity may delegate the responsibility of providing the required notifications to the business associate that suffered the breach or to another of its business associates. 45 CFR § 164.410.

Summary of Breach Reports

This report describes the types and numbers of breaches reported to the Office for Civil Rights (OCR) (the office within the Department that is responsible for administering and enforcing the HIPAA Privacy, Security, and Breach Notification Rules) that occurred between January 1, 2011, and December 31, 2012, as well as provides some cumulative data on breaches reported since the September 23, 2009, effective date of the breach notification requirements. The report also describes actions that have been taken by covered entities and business associates in response to the reported breaches.

In addition, this report generally describes the OCR investigations and enforcement actions with respect to the reported breaches. OCR opens compliance reviews to investigate all reported breaches affecting 500 or more individuals, and may open compliance reviews into certain reported breaches affecting fewer than 500 individuals. As discussed in greater detail below, as of the date of this report, the Department has entered into seven resolution agreements/corrective action plans totaling more than $8 million in settlements as a result of investigations conducted after a breach incident was reported to the Department.

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 236 reports of these larger breaches that occurred in calendar year 2011[3], which affected a total of approximately

[3] The Department receives some reports where the breach occurred over the period of several years. For the purposes of this report, breach incidents spanning multiple years are included with the data for the last year in which the breach occurred, e.g., a breach incident that continued from 2009 to 2012 would be reported with the 2012 numbers.

11,415,185 individuals.[4,5] For breaches occurring in calendar year 2012, OCR received 222 reports of these larger breaches, which affected a total of approximately 3,273,735 individuals. Cumulatively, from September 23, 2009, to December 31, 2012, OCR received 710 reports affecting a total of approximately 22.5 million individuals.

The 2009/2010 Annual Report to Congress[6] identified four primary reported causes of larger breaches of unsecured PHI for 2009: Theft; Intentional Unauthorized Access, Use or Disclosure; Human Error; and Loss. For 2010, a fifth category was reported for Improper Disposal. For breaches occurring in 2011 and 2012, based on changes in the Department's breach reporting system, this report categorizes breaches into the following categories of reported causes: Theft; Loss; Unauthorized Access/Disclosure; Improper Disposal; Hacking/IT Incident; and Unknown/Other (capturing breaches attributable to other causes or breaches where the cause is unknown). Given the variation in some of the categories across the reporting years, the two cumulative charts that follow covering the years 2009-2012 identify the percentage of breach reports that indicated the cause of breach was due either to Theft, Loss, or Unauthorized Access/Disclosure. Breach reports submitted under all other categories of causes have been collapsed into an "Other" category for purposes of the 2009-2012 charts. For the charts covering only the years 2011 and 2012, all six categories of causes of breaches are included. [7]

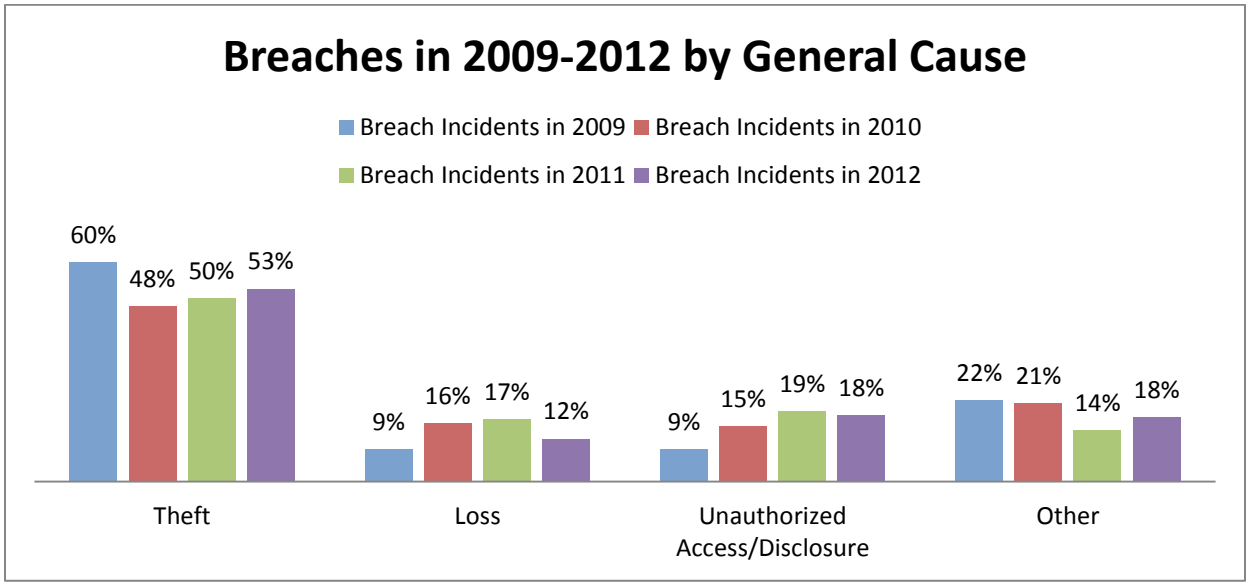
[4] The numbers of affected individuals provided throughout this report are approximate because some covered entities reported uncertainty about the number of records affected by a breach.

[5] The year 2011 was atypical in terms of the number of individuals affected by larger breaches, due to multiple reports of breaches in 2011 each affecting more than one million individuals, including one particularly large breach affecting nearly five million individuals and another large breach affecting nearly two million individuals. More details on these breaches can be found in the section "Largest breaches in 2011 for each reported cause" beginning on page 11.

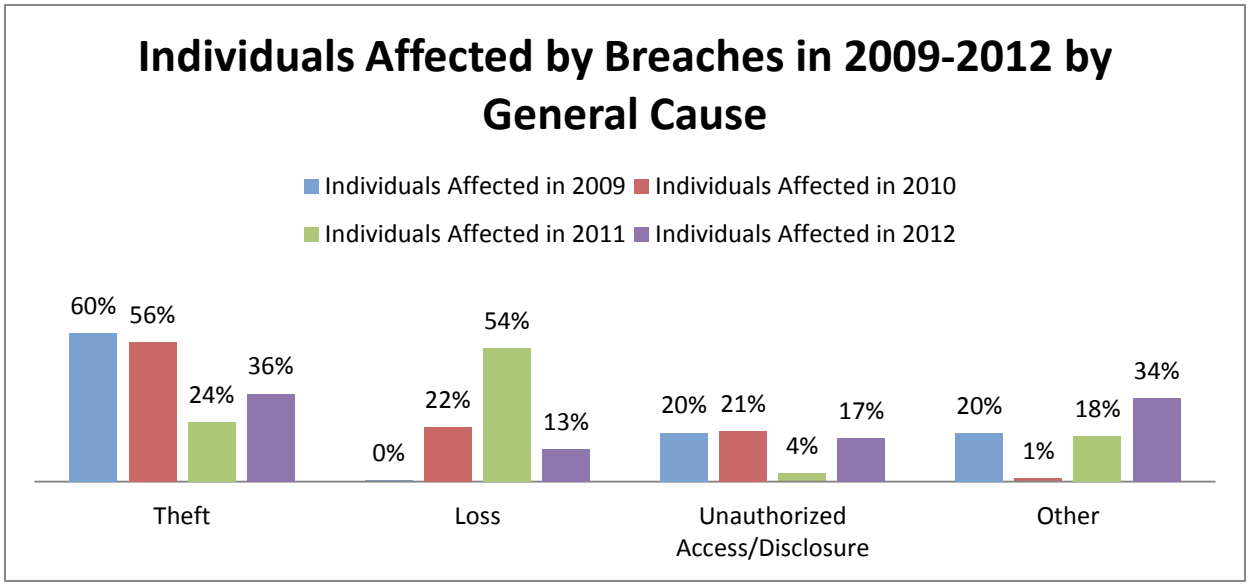
[6] See the Annual Report to Congress on Breaches of Unsecured Protected Health Information For Calendar Years 2009 and 2010, available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachrept.pdf.

[7] In some cases, covered entities indicated multiple causes that contributed to the breach incident. For the purposes of this report, breach incidents are categorized by only the most specific cause listed by the covered entity, e.g., a breach listed as both a "theft" and an "unauthorized access/disclosure" has been categorized as a "theft" for the purposes of this report.

The following chart shows the percentage of breaches in 2009-2012 categorized by four general causes of breaches.[8]

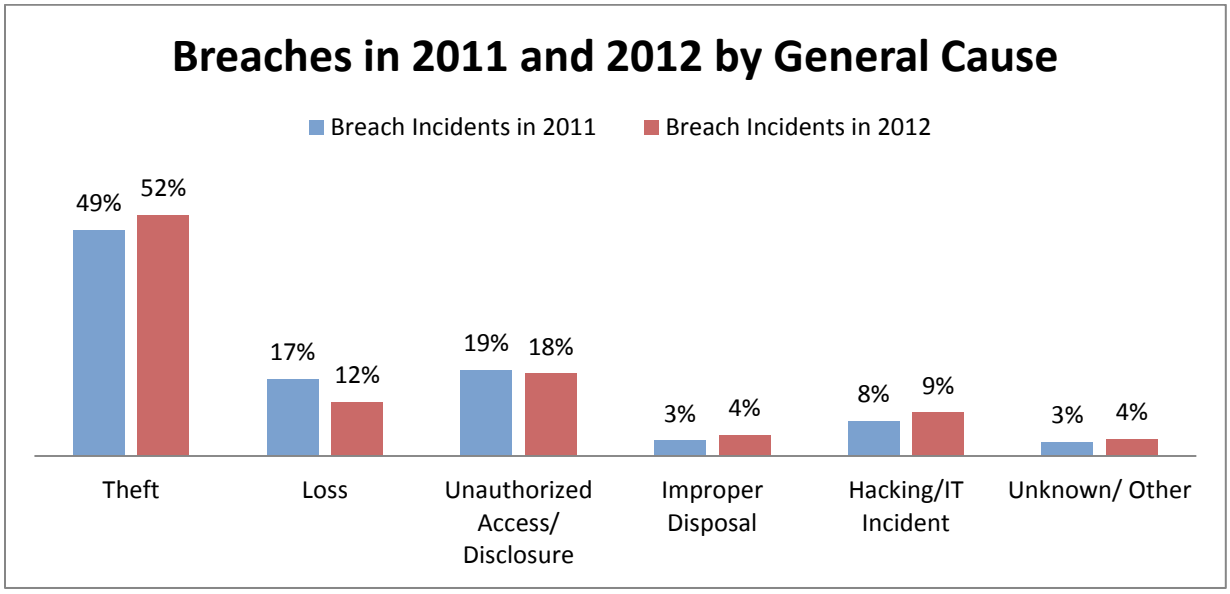


The following chart shows the percentage of individuals affected by breaches in 2009 – 2012 by four general causes of breaches.

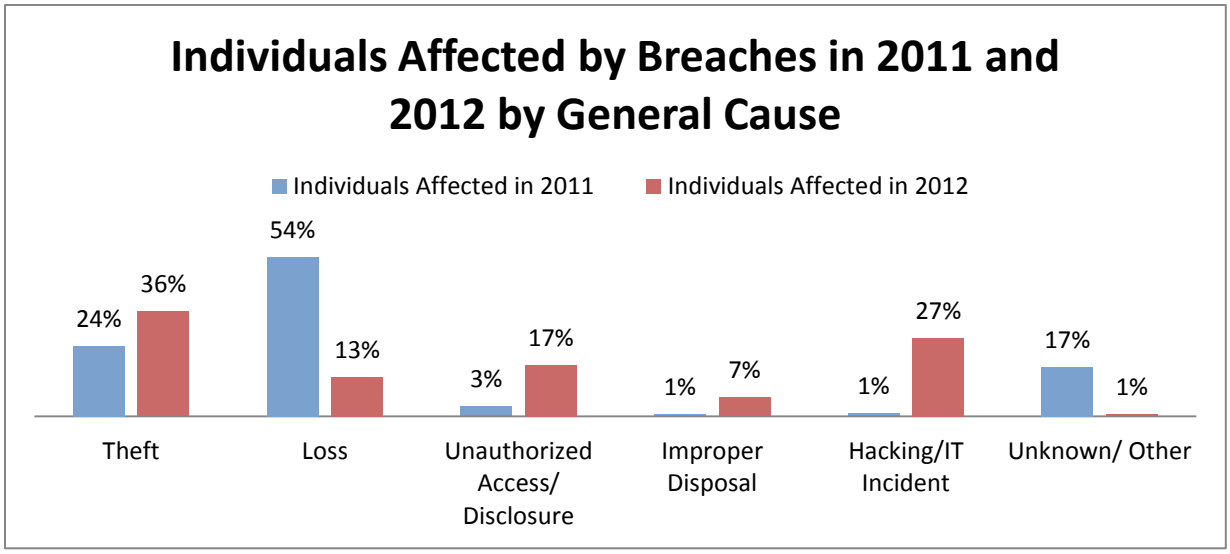


[8] All percentages shown in the charts in this report are rounded to the nearest whole number and, therefore, may not add up to 100% in all cases.

The following chart shows the percentage of breaches in 2011 and 2012 categorized by six general causes of breaches.

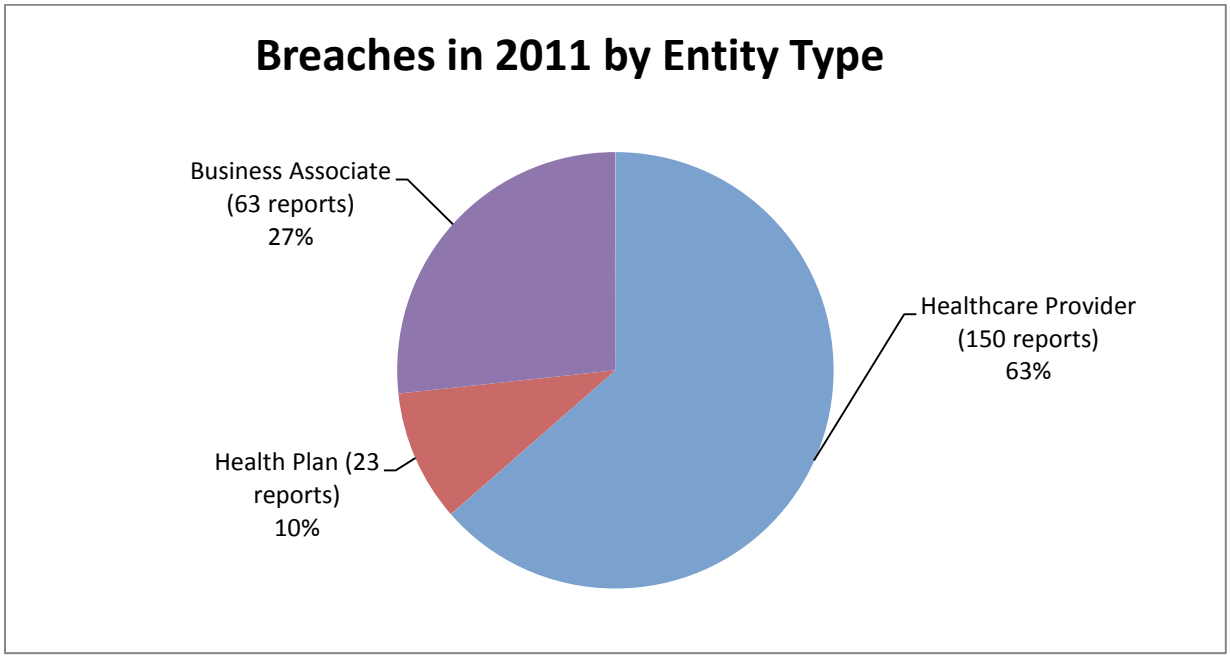


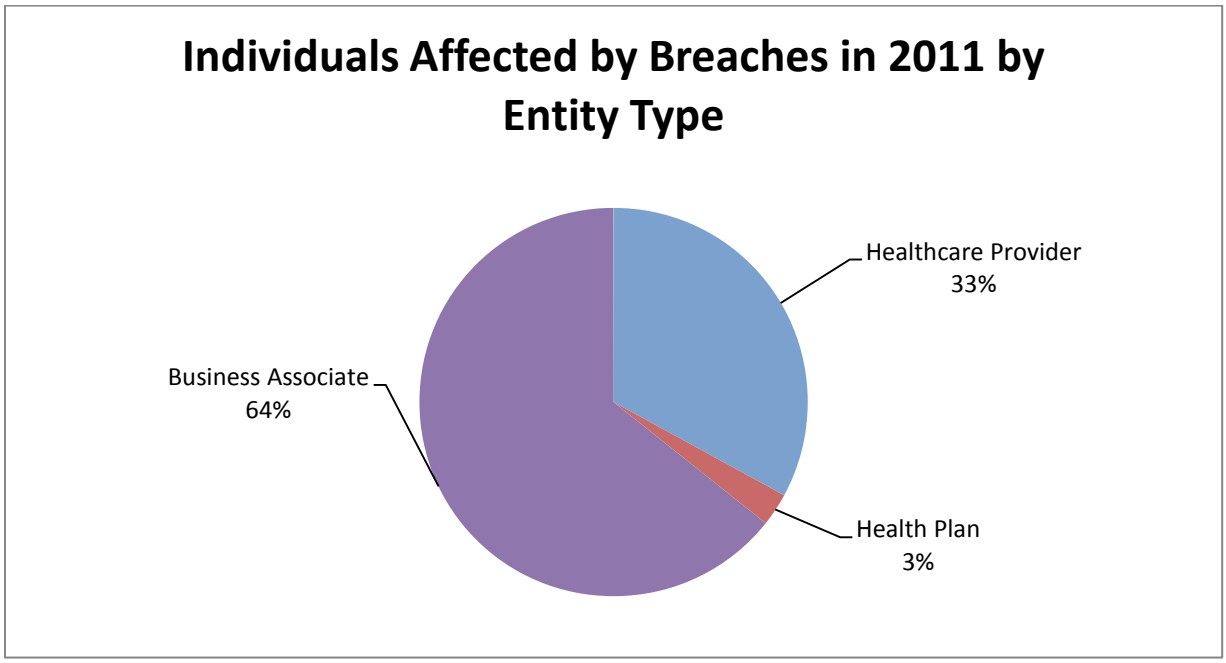
The following chart shows the percentage of individuals affected by breaches in 2011 and 2012 by six general causes of breaches.



Breaches in 2011 Affecting 500 or More Individuals

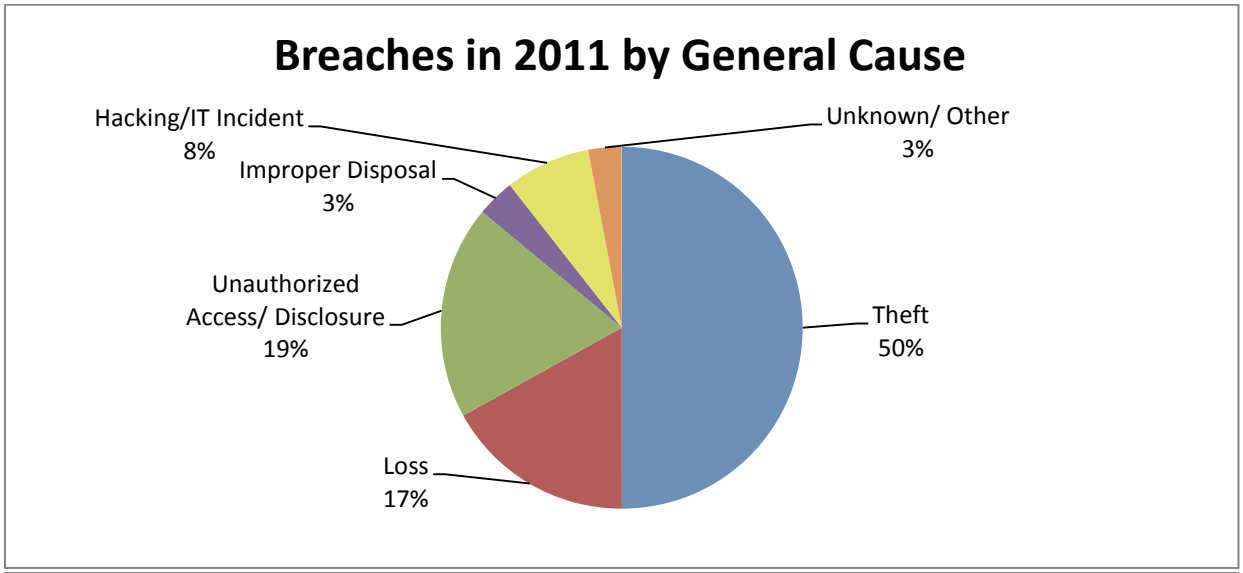
For the 236 breaches in 2011 affecting 500 or more individuals, OCR received 150 reports of breaches at healthcare providers (affecting a total of 3,763,041 individuals), 23 reports of breaches at health plans (affecting a total of 313,379 individuals), and 63 reports of breaches at business associates (affecting a total of 7,338,765 individuals). OCR did not receive any reports of breaches at healthcare clearinghouses in 2011.

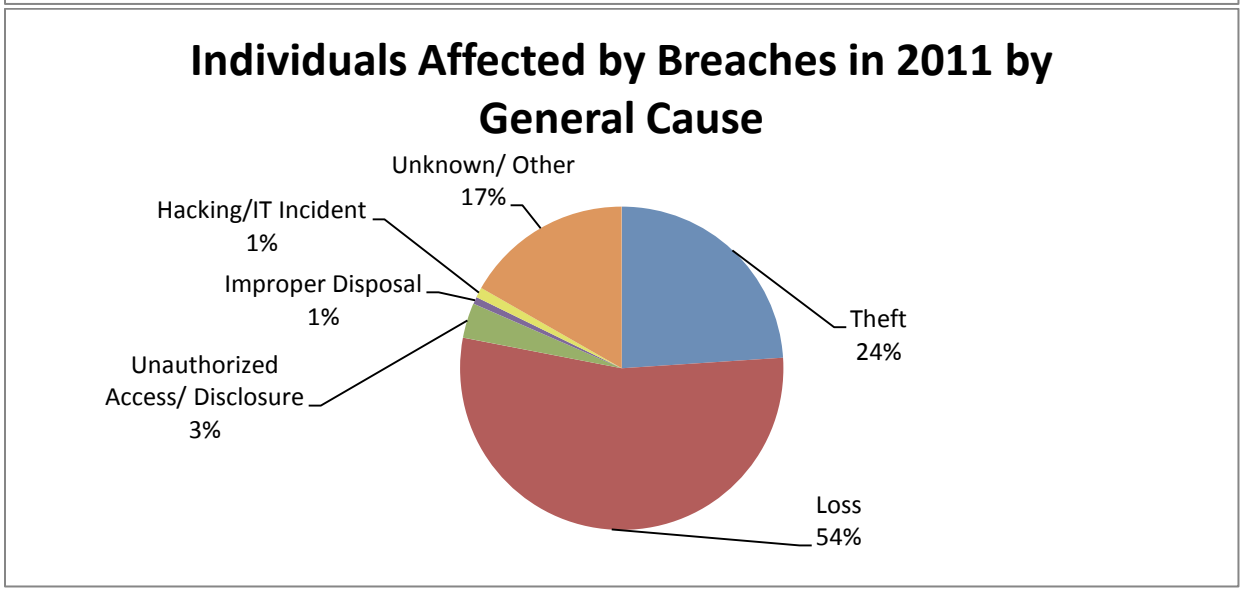




The 236 reports for breaches occurring in 2011 can be categorized by six general causes of incidents as follows (in order of frequency):

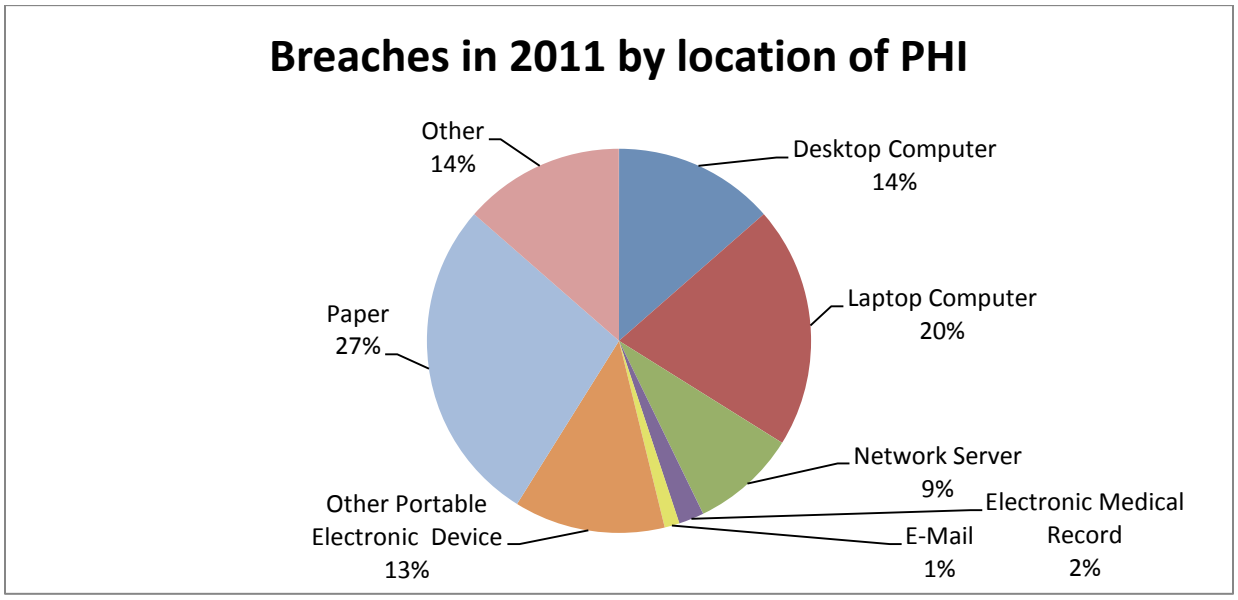
(1) theft of electronic equipment/portable devices or paper containing PHI (118 reports affecting 2,735,416 individuals);
(2) unauthorized access or disclosure of records containing PHI (45 reports affecting 399,738 individuals);
(3) loss of electronic media or paper records containing PHI (40 reports affecting 6,173,012 individuals);
(4) hacking/IT incident of electronic equipment or a network server (18 reports affecting 115,900 individuals);
(5) improper disposal of PHI (8 reports affecting 80,054 individuals); and
(6) unknown/other causes of breaches of PHI (7 reports affecting 1,911,065 individuals).



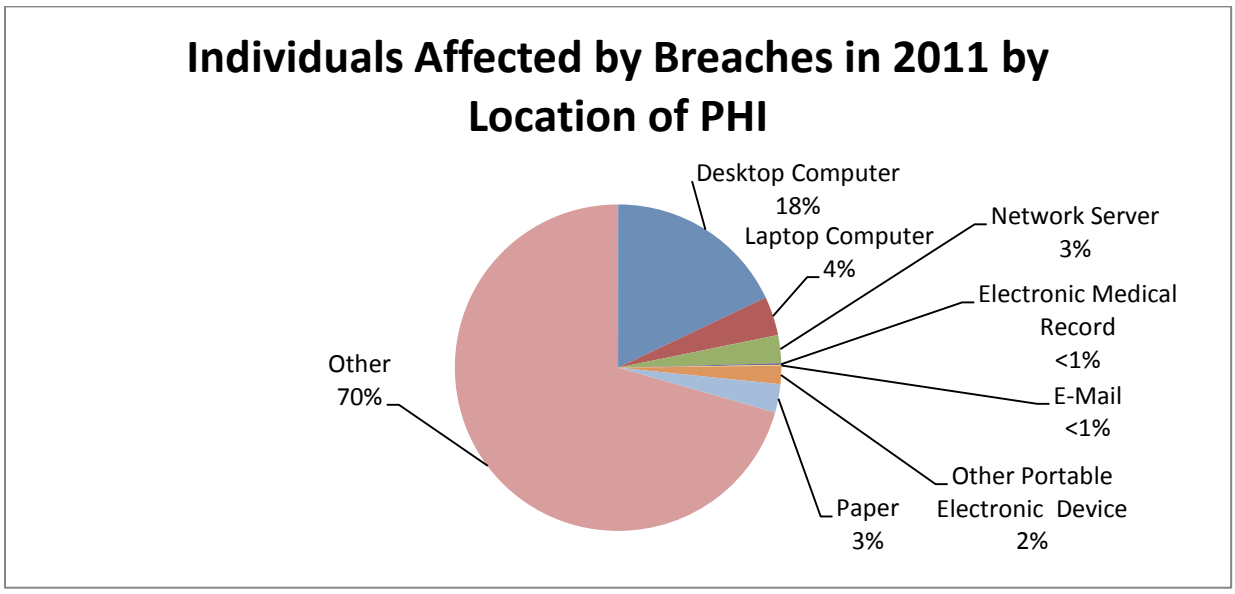


The 236 reports for breaches occurring in 2011 described the following locations of the PHI (in order of frequency):[9]

(1) paper (65 reports affecting 321,731 individuals);
(2) laptop computer (48 reports affecting 437,770 individuals);
(3) other (32 reports affecting 8,054,479 individuals);
(4) desktop computer (32 reports affecting 2,049,875 individuals);
(5) other portable electronic device (30 reports affecting 206,802 individuals);
(6) network server (21 reports affecting 316,163 individuals);
(7) electronic medical record (5 reports affecting 19,423); and
(8) e-mail (3 reports affecting 8,942 individuals).



[9] While covered entities sometimes list multiple locations of PHI, for the purposes of this report, each breach incident has been included in only one location category. When multiple categories were selected and a primary location could be determined, the primary location was used for the purpose of this report. When a breach incident affected multiple locations of PHI, e.g., a natural disaster that led to the destruction or loss of all electronic and paper records, such breach incidents are listed with "other" as the location.



Largest breaches in 2011 for each reported cause

This section describes the largest breach, by number of individuals affected, for each of the six reported causes of breaches, followed by a short summary of other scenarios reported for each cause.

The largest breach in 2011 was the result of a loss of back-up tapes by a business associate and affected approximately 4.9 million individuals. The back-up tapes contained individuals' PHI captured from 1992 through 2011. Other incidents reported as a loss of PHI involved paper records, USB drives, hard drives, microfilms, and other media that could not be located or that were lost in transit or shipping.

The largest breach reported as a theft in 2011 involved an unencrypted desktop computer stolen from a covered entity's facility during a burglary, which contained the PHI of just under 1 million individuals. In most reported theft cases, laptop computers, desktop computers, and other portable electronic devices, such as hard drives and USB drives, either were stolen from a covered entity's facility during a break-in that occurred after the entity's regular business hours, or from an employee's vehicle.

The largest breach reported with an unknown cause in 2011 affected 1.9 million individuals and involved missing hard drives associated with the covered entity's corporate servers. Other breaches in 2011 reported with an unknown cause include a provider who failed to secure all PHI when relocating to another location and could not locate the PHI left behind, and hard drives that were discovered missing, among other causes.

The largest breach in 2011 involving the unauthorized disclosure of PHI occurred when letters were mailed to individuals with the envelope displaying all or part of the individuals' member ID numbers, dates of birth, and medications. This breach affected 175,350 individuals. Other

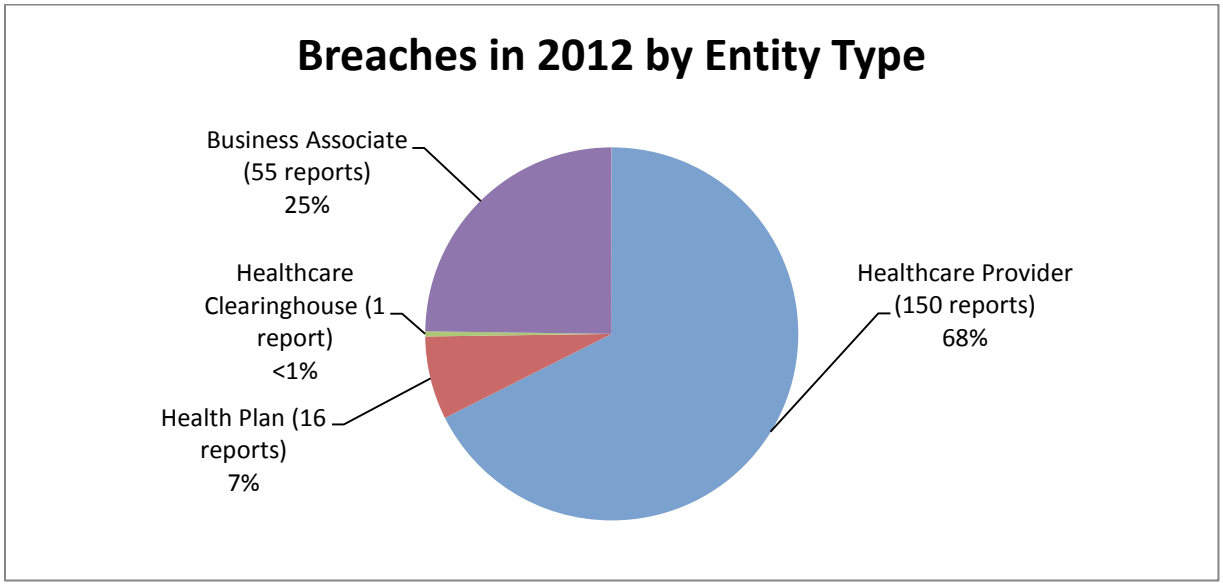
reports of unauthorized access or disclosure of PHI involved mailing errors, as well as employees viewing or removing PHI for purposes beyond the scope of their duties.

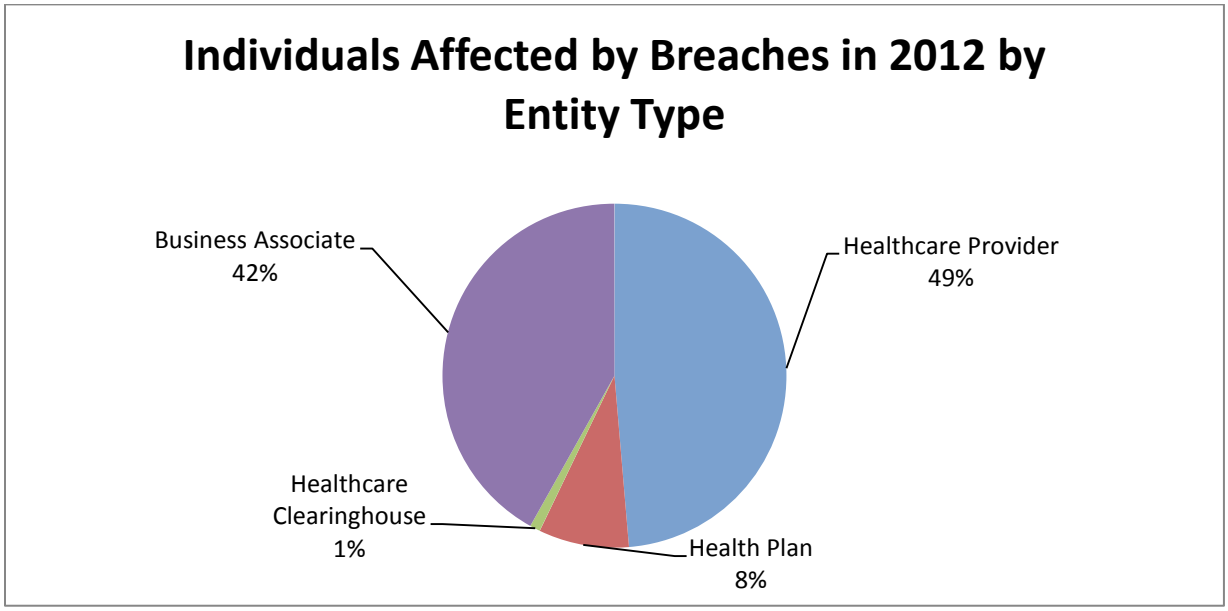
The largest improper disposal breach for 2011 involved the disposal of a network server and affected approximately 55,000 individuals. In this case, the covered entity reported that the room that housed the network server was flooded during Hurricane Lee and the restoration company with which the covered entity had contracted improperly disposed of the server. Most of the improper disposal cases involving paper records were the result of an employee mistakenly putting medical records in the trash or recycling bins rather than the covered entity's shred bins.

The largest hacking/IT incident for 2011, affecting approximately 42,000 individuals, involved a former employee's log-in information being used to log-in and delete files. Other hacking/IT incidents involved covered entities that discovered computer viruses or malware, and a covered entity that discovered an unknown person uploaded a file containing PHI to a public website.

Breaches in 2012 Affecting 500 or More Individuals

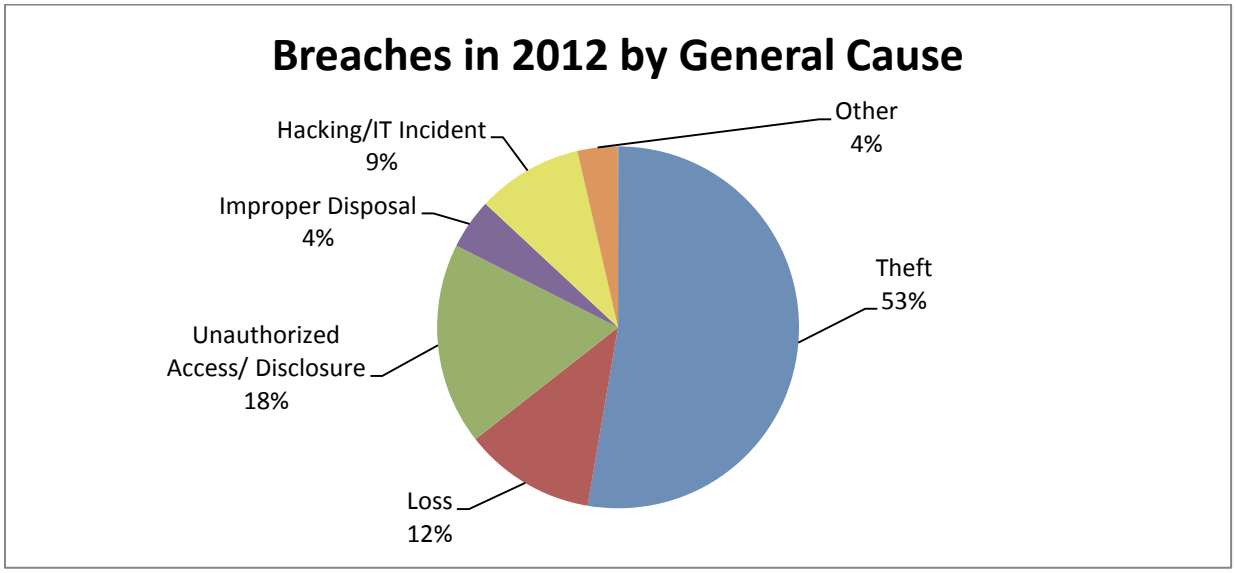
For breaches affecting 500 or more individuals in 2012, OCR received 150 reports of breaches at healthcare providers (affecting a total of 1,592,558 individuals), 55 reports of breaches at business associates (affecting a total of 1,370,880 individuals), 16 reports of breaches at health plans (affecting a total of 278,297 individuals), and 1 report of a breach at a healthcare clearinghouse (affecting 32,000 individuals).

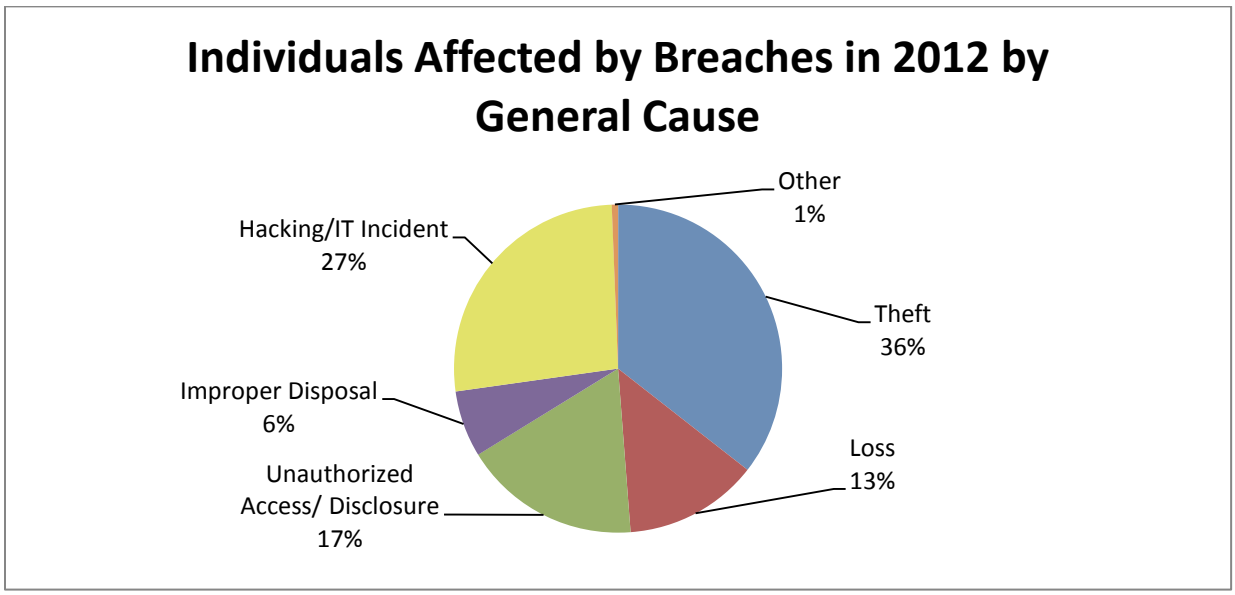




The 222 reports submitted to OCR for breaches occurring in 2012 can be categorized by six general causes of incidents as follows (in order of frequency):

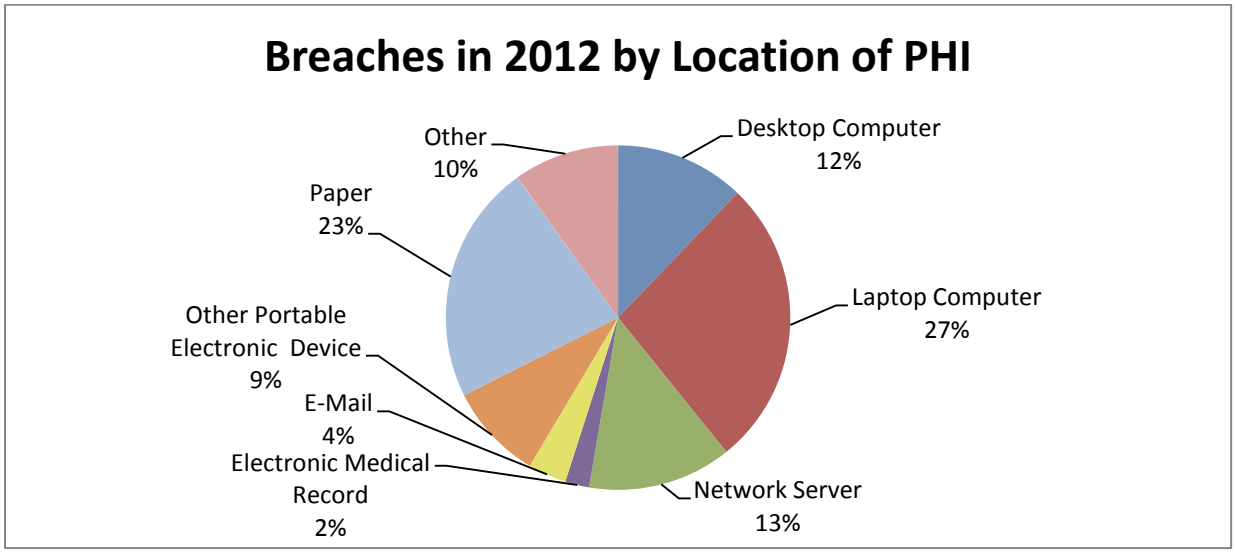
(1) theft of electronic equipment/portable devices or paper containing PHI (117 reports affecting 1,164,452 individuals);
(2) unauthorized access or disclosure of records containing PHI (40 reports affecting 571,445 individuals);
(3) loss of electronic media or paper records containing PHI (26 reports affecting 432,148 individuals);
(4) hacking/IT incident of electronic equipment or a network server (21 reports affecting 870,871 individuals);
(5) improper disposal of PHI (10 reports affecting 214,601 individuals); and
(6) other causes of breaches of PHI (8 reports affecting 20,218 individuals).

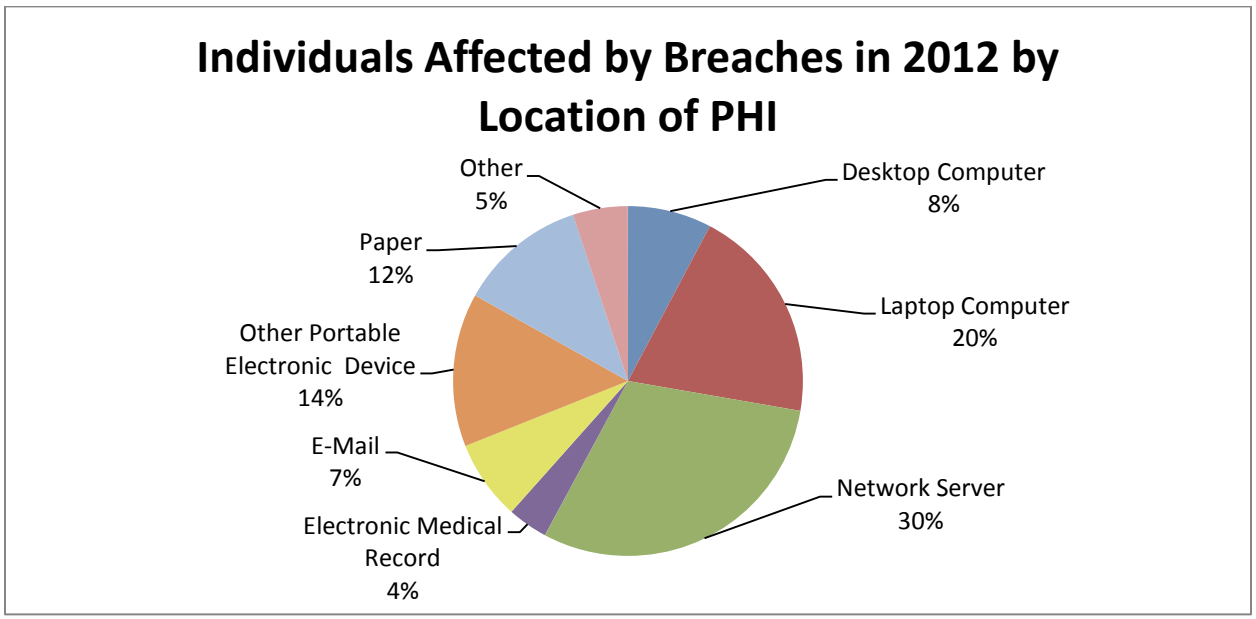




The 222 reports submitted to OCR for breaches occurring in 2012 described the following locations of the PHI (in order of frequency):

(1) laptop computer (60 reports affecting 654,158 individuals);
(2) paper (50 reports affecting 386,065 individuals);
(3) network server (30 reports affecting 986,607 individuals);
(4) desktop computer (27 reports affecting 253,720 individuals);
(5) other (22 reports affecting 166,411 individuals);
(6) other portable electronic device (20 reports affecting 463,702 individuals);
(7) e-mail (8 reports affecting 241,108 individuals); and
(8) electronic medical record (5 reports affecting 121,964 individuals).





Largest breaches in 2012 for each reported cause

This section describes the largest breach, by number of individuals affected, for each of the six reported causes of breaches, followed by a short summary of other scenarios reported for each cause.

The largest breach in 2012 resulting from theft involved an unencrypted laptop that was stolen from an employee's personal vehicle. This incident affected 116,506 individuals. Other reports of theft of PHI reported for 2012 involved thefts of laptops and other portable electronic devices from employees' vehicles, thefts of back-up tapes and paper records from offices and in transit, a stolen controlled substance log from a pharmacy, clinical research records stolen from an employee's vehicle, and a box of patient records stolen from a storage facility, among other incidents.

The largest breach in 2012 resulting from a hacking/IT incident was also the largest breach in 2012. The incident involved an unencrypted network server containing PHI for approximately 780,000 individuals that was compromised by a cyber-attack. Other hacking/IT incidents involved covered entities that discovered viruses or malware, or unidentified, unauthorized persons obtaining access to systems. In an additional incident, a covered entity discovered that files containing PHI were corrupt and inaccessible, and later received a "ransom note" to restore access to the files.

The largest breach in 2012 involving the unauthorized access or disclosure of PHI affected 228,435 individuals. In this case, an employee of the covered entity impermissibly accessed reports involving Medicaid recipients and other individuals for just over a two month period, and sent these reports, unencrypted, to the employee's personal email. In another incident, a covered entity was informed by local law enforcement during a police investigation that paper records

containing PHI from the covered entity were found in the possession of a third party. The incident affected approximately 64,846 individuals.

The largest breach in 2012 reported as having an "other" cause involved a covered entity that due to a computer programming error mailed PHI to individuals' old addresses. This breach affected approximately 7,039 individuals. The other breaches reported with an "other" cause involved misdirected mailings of paper records to the wrong recipient.

The largest reported incident in 2012 involving improper disposal resulted from the improper disposal of paper records after a business associate was hired to digitize and destroy x-rays and accompanying paper jackets containing the PHI of 189,489 individuals, but later disappeared with the x-rays. Other improper disposal breaches involved paper records containing PHI disposed of in recycling or trash bins rather than shred bins.

The largest breach reported as a loss in 2012 involved a missing laptop from a physician's office. This incident affected approximately 17,000 individuals. Other incidents involving the loss of PHI in 2012 involved missing unencrypted backup tapes, unencrypted USB drives, and paper records from a healthcare provider's office, as well as records lost as a result of a natural disaster, such as a hurricane or tornado, among others.

Remedial Action Reported

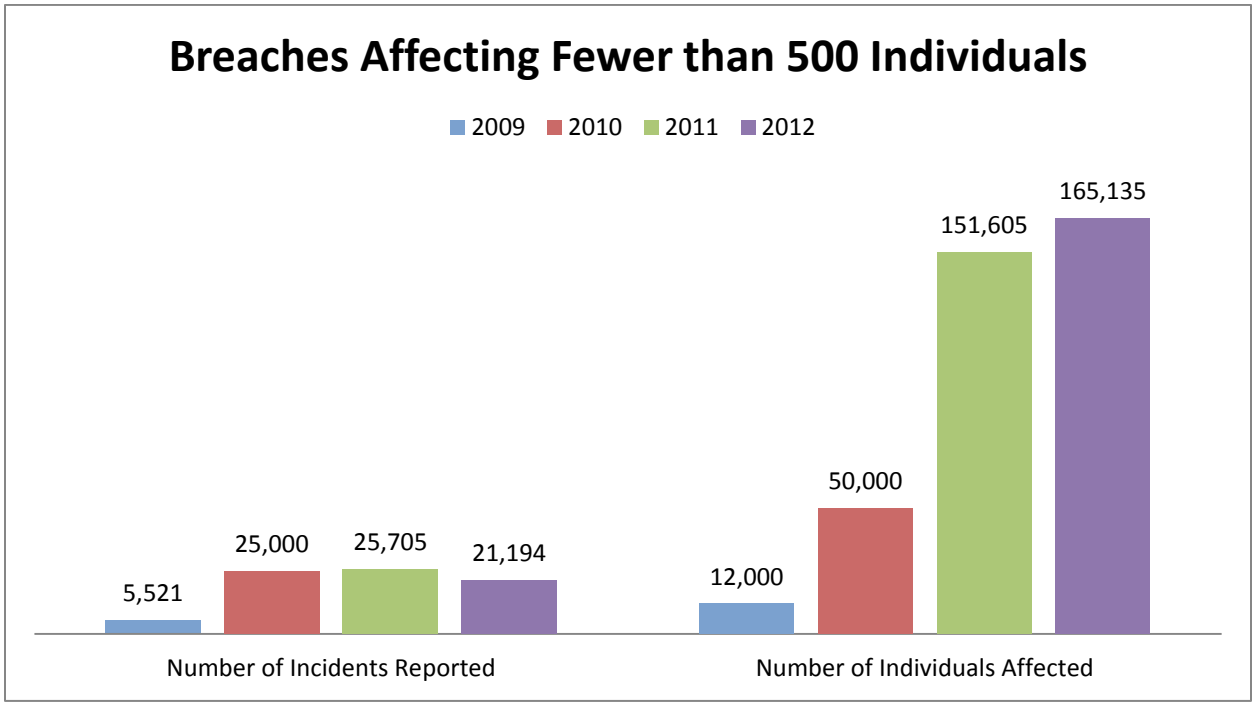
For breaches affecting 500 or more individuals that occurred in 2011 and 2012, in addition to providing the required notifications, covered entities most commonly reported taking one or more of the following steps to mitigate the potential consequences of the breaches and prevent future breaches:

- 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 PHI;
- Providing free credit monitoring to customers;
- Adopting encryption technologies;
- Imposing sanctions on workforce members who violated policies and procedures for removing PHI from facilities or who improperly accessed PHI, among other issues;
- Changing passwords;
- Performing a new risk assessment; and

- Revising business associate contracts to include more detailed provisions for the protection of health information.

Breaches Involving Fewer than 500 Individuals

A covered entity must notify OCR of breaches involving fewer than 500 individuals no later than 60 days after the end of the calendar year in which the breaches are discovered. For breaches discovered during 2011, notification to OCR was required no later than March 1, 2012. For breaches discovered during 2012, notification to OCR was required no later than March 1, 2013.

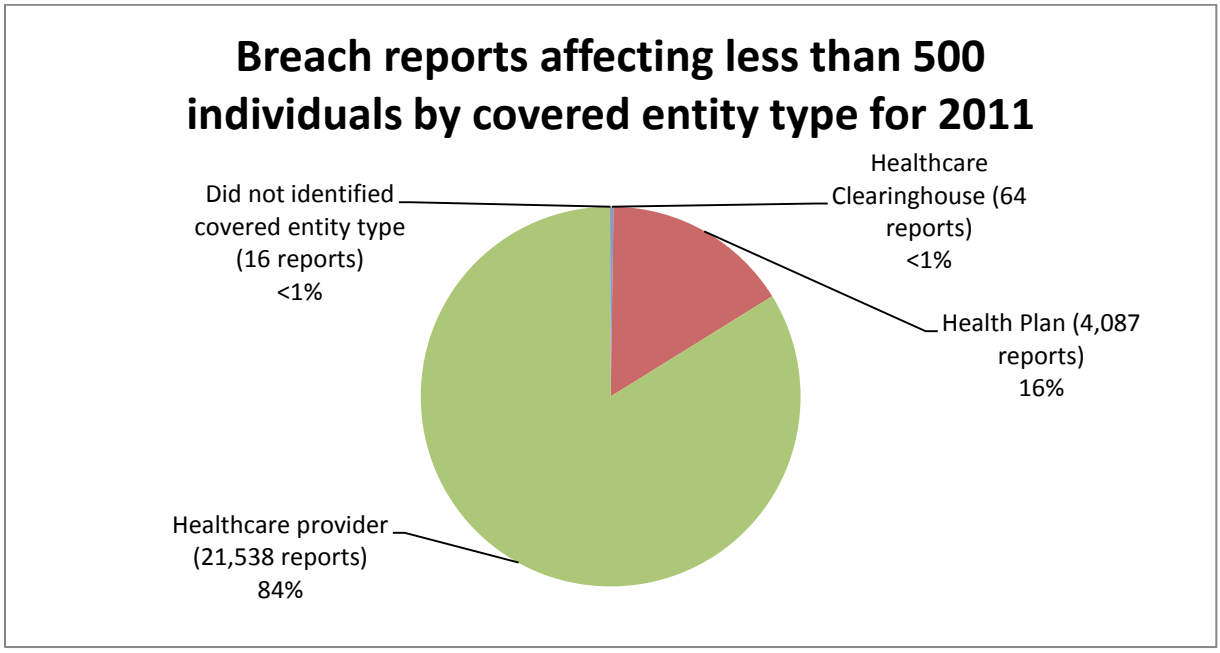


This chart represents the number of incidents reported to OCR and the number of individuals affected by those incidents, by the year the breach occurred for the past four years. The 2009 numbers reflect breaches reported to OCR that occurred between September 23, 2009 (the effective date of the breach notification regulations) and December 31, 2009.

Breaches involving less than 500 individuals for 2011

OCR received approximately 25,705 reports of smaller breaches that occurred between January 1, 2011, and December 31, 2011. These smaller breaches affected approximately 151,605 individuals. Of these reports of smaller breaches, 4,087 were reported by health plans (affecting 28,459 individuals), 21,538 were reported by healthcare providers (affecting 122,467

individuals), and 64 were reported by healthcare clearinghouses (affecting 479 individuals).[10] Sixteen breach reports (affecting 200 individuals) did not identify the type of covered entity.



The most common causes of breach incidents (in order of frequency) for breaches affecting less than 500 individuals were:

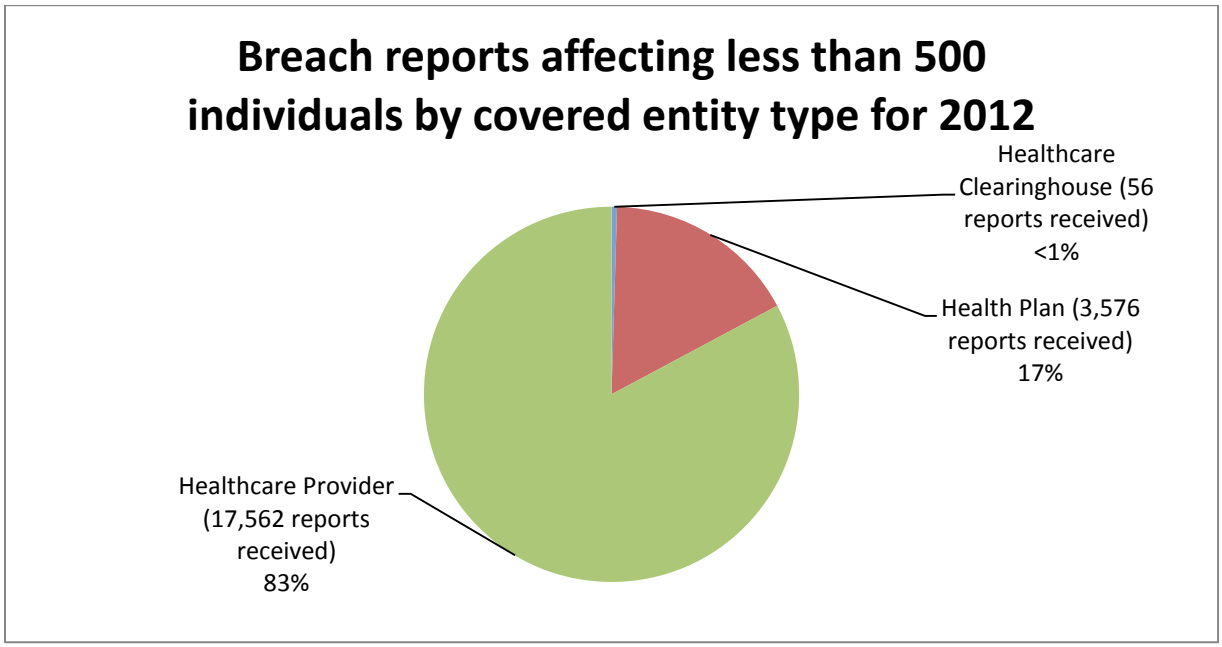
(1) unauthorized access or disclosure (21,639 reports affecting 62,069 individuals);
(2) unknown/other (2,033 reports affecting 13,091 individuals);
(3) theft (1,028 reports affecting 49,132 individuals);
(4) loss (789 reports affecting 20,176 individuals);
(5) improper disposal (155 reports affecting 4,518 individuals); and
(6) hacking/IT incident (61 reports affecting 2,619 individuals).

Of these reports, 15,878 reports involved paper records, 1,758 reports involved an electronic medical record, 584 reports involved desktop computers, 451 reports involved e-mail, 402 reports involved portable electronic devices, 245 reports involved laptops, and 6,105 reports did not identify the location of the data that was breached.

Breaches involving less than 500 individuals for 2012

OCR received approximately 21,194 reports of smaller breaches that occurred between January 1, 2012, and December 31, 2012. These smaller breaches affected approximately 165,135 individuals. Of these reports of smaller breaches, 3,576 were reported by health plans (affecting 27,617 individuals), 17,562 were reported by health care providers (affecting 136,743 individuals), and 56 were reported by health care clearinghouses (affecting 775 individuals).

[10] Information on breaches that occurred at a business associate is not available as a category separate from covered entity type for the breaches affecting fewer than 500 individuals, as it is for breaches involving 500 or more individuals.



The most common causes of breach incidents (in order of frequency) for breaches affecting less than 500 individuals were:

(1) unauthorized access or disclosure (15,695 reports affecting 58,882 individuals);
(2) unknown/other (2,945 reports affecting 19,483 individuals);
(3) theft (1,063 reports affecting 50,272 individuals);
(4) loss (774 reports affecting 19,518 individuals);
(5) hacking/IT incident (514 reports affecting 10,534 individuals); and
(6) improper disposal (203 reports affecting 6,446 individuals).

Of these reports, 12,946 reports involved paper records, 1,694 reports involved an electronic medical record, 711 reports involved desktop computers, 562 reports involved e-mail, 299 reports involved portable electronic devices, 220 reports involved laptops, and 4,398 reports did not identify the location of the data that was breached.

Details on Breaches involving less than 500 individuals for 2011 and 2012

Several incidents reported for 2011 and 2012 involved misdirected communications, including incidents where the clinical or claims record of one individual was mistakenly mailed or faxed to another individual, test results were sent to the wrong patient, files were attached to the wrong patient record, emails were sent to the wrong individuals, and member ID cards were mailed to the wrong individuals. In response to these incidents, covered entities commonly reported taking remedial actions such as fixing "glitches" in software that incorrectly compiled lists of patient names and contact information, revising policies and procedures, and training or retraining employees who handle PHI.

Cases Investigated and Action Taken

OCR has opened investigations into all of the 458 breaches affecting 500 or more individuals that occurred in 2011 and 2012. OCR has also opened a number of investigations into breaches affecting fewer than 500 individuals. As of the date of this report, OCR has over 500 open investigations that were opened as the result of a breach report. OCR has closed investigations resulting from breach reports after achieving voluntary compliance, through corrective action and technical assistance, through resolution agreements, and as no violation.

Enforcement Actions

As of the end of 2013, OCR has entered into resolution agreements with seven covered entities as the result of investigations opened in response to breach reports submitted to OCR for breaches that occurred through the end of 2012. These resolution agreements represent the first settlements with OCR from investigations into reported breaches. All of these breaches affected 500 or more individuals, except for the breach involving the Hospice of North Idaho, which affected 441 individuals, as noted below. Most of these breach incidents occurred in 2009 and 2010.[11] Under these resolution agreements, covered entities agreed to pay more than $8 million to the government. Nearly two million individuals were affected by the breaches that led to these investigations. Four of these cases, including one stemming from a breach incident affecting less than 500 individuals, involved the theft of laptops or other electronic devices containing unsecured electronic protected health information (ePHI). In addition to the resolution agreements and settlement amounts, OCR has entered into corrective action plans (CAPs) requiring action on the part of the covered entities, including requiring efforts to retrieve missing PHI, reviewing and correcting deficiencies in Privacy Rule and Security Rule compliance, and submitting certain reports to OCR. These cases are discussed in greater detail below.

Resolution Agreement with Blue Cross Blue Shield of Tennessee

OCR opened an investigation after receiving a breach report from Blue Cross Blue Shield of Tennessee (BCBST) indicating that 57 unencrypted computer hard drives were stolen from a leased facility in Tennessee. The hard drives contained the PHI of over 1 million individuals, including member names, social security numbers, diagnosis codes, dates of birth, and health plan identification numbers. OCR's investigation revealed that BCBST failed to implement appropriate administrative safeguards to adequately protect information remaining at the leased facility by not performing the required security evaluation in response to operational changes. In addition, the investigation showed a failure to implement appropriate physical safeguards by not having adequate facility access controls. Both of these safeguards are required by the HIPAA Security Rule.

[11] Because the resolution agreements for these incidents were not entered into until 2012 or 2013, they were not discussed in the Annual Report to Congress on Breaches of Unsecured Protected Health Information for Calendar Years 2009 and 2010.

On March 9, 2012, the Department reached an agreement with BCBST to settle the potential violations of the Privacy and Security Rules. The enforcement action was the first resulting from a breach report.

Under the resolution agreement, BCBST agreed to pay a $1,500,000 resolution amount and implement a strong CAP that includes:

- reviewing, revising, and maintaining its HIPAA Privacy and Security policies and procedures;
- conducting regular and robust HIPAA trainings for all BCBST employees; and
- engaging a monitor to perform reviews to ensure BCBST compliance with the corrective action plan.

Resolution Agreement with the Alaska Department of Health and Social Services

OCR began its investigation following a breach report submitted by the Alaska Department of Health and Social Services (Alaska DHSS). The report indicated that a portable electronic storage device (USB hard drive) possibly containing ePHI was stolen from the vehicle of an Alaska DHSS employee. Over the course of the investigation, OCR found evidence that the Alaska DHSS did not have adequate policies and procedures in place to safeguard ePHI. Further, the evidence indicated that DHSS had not completed a risk analysis, implemented sufficient risk management measures, completed security training for its workforce members, implemented device and media controls, or addressed device and media encryption as required by the HIPAA Security Rule.

On June 25, 2012, the Department reached an agreement with the Alaska DHSS to settle potential violations of the HIPAA Security Rule. To resolve the Department's investigation, Alaska DHSS agreed to pay $1,700,000 and to take corrective action to properly safeguard the ePHI of its Medicaid beneficiaries.

Under the CAP, Alaska DHSS agreed to:

- developing, retaining, and revising its HIPAA Privacy and Security policies and procedures as necessary;
- conducting and documenting a risk analysis that complies with the HIPAA Security Rule;
- developing a risk management plan, as required by the HIPAA Security Rule, to address the risks identified by the risk analysis;
- training workforce members on the requirements of the HIPAA Rules; and
- engaging a qualified, independent third-party monitor to, among other duties, conduct compliance reviews, and render reports to the Department for a period of three years.

Resolution Agreement with Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates Inc.

Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates Inc. (collectively referred to as "MEEI") submitted a breach report to OCR reporting the theft of an unencrypted personal laptop containing the ePHI of MEEI patients and research subjects. The information contained on the laptop included patient prescriptions and clinical information. OCR's investigation revealed that MEEI failed to comply with certain requirements of the Security Rule, including conducting a thorough analysis of the risk to ePHI maintained on portable devices, adopting and implementing policies and procedures to restrict access to ePHI to authorized users of portable devices, and adopting and implementing policies and procedures to address security incident identification, reporting, and response. OCR's investigation indicated that these failures continued over an extended period of time, demonstrating a long-term, organizational disregard for the requirements of the Security Rule.

On September 13, 2012, the Department reached an agreement with MEEI to settle potential violations of the HIPAA Security Rule. To resolve the Department's investigation, MEEI agreed to pay $1,500,000 and to take corrective action to properly safeguard the ePHI of its patients, which includes:

- developing, retaining, and revising its HIPAA Privacy and Security policies and procedures as necessary;
- conducting and documenting a risk analysis that complies with the HIPAA Security Rule;
- developing a risk management plan, as required by the HIPAA Security Rule, to address the risks identified by the risk analysis;
- identifying a security official who is responsible for the development and implementation of the policies and procedures and the HIPAA Security Rule;
- training workforce members on the requirements of the HIPAA Rules; and
- engaging a qualified, independent third-party monitor to, among other duties, conduct compliance reviews, and render reports to the Department for a period of three years.

Resolution Agreement with the Hospice of North Idaho

OCR began its investigation after Hospice of North Idaho (HONI) reported to OCR that an unencrypted laptop computer containing the ePHI of 441 patients had been stolen in June 2010. Laptops containing ePHI are regularly used by the organization as part of its field work. Over the course of the investigation, OCR discovered that HONI had not conducted a risk analysis to safeguard ePHI. Further, HONI did not have in place policies or procedures to address mobile device security as required by the HIPAA Security Rule. Since the June 2010 theft, HONI has

taken extensive additional steps to improve their HIPAA Privacy and Security compliance program.

On December 31, 2012, the Department reached agreement with HONI to settle potential violations of the HIPAA Security Rule. To resolve the Department's investigation, HONI agreed to pay $50,000 and to take corrective action to properly safeguard the ePHI of its patients, including reporting certain incidents to the Department for a two-year period.

Resolution Agreement with Idaho State University

OCR began an investigation following a breach report submitted by Idaho State University (ISU), reporting the breach of unsecured ePHI. OCR's investigation indicated that ISU's risk analyses and assessments of its clinics were incomplete and inadequately identified potential risks or vulnerabilities. ISU also failed to implement sufficient security measures to reduce risks and vulnerabilities. As a result, the ePHI of approximately 17,500 individuals was unsecured for approximately 10 months, due to the disabling of firewall protections at servers maintained by ISU.

On May 13, 2013, the Department reached an agreement with ISU to settle potential violations of the HIPAA Security Rule. To resolve the Department's investigation, ISU agreed to pay $400,000 and to take corrective action to properly secure the ePHI of its patients, which includes:

- providing OCR with documentation of its designation as a hybrid entity;
- providing OCR with its risk management plan to reduce the security risks and vulnerabilities;
- providing OCR with documentation of implementation of its policies and procedures regarding information system activity review;
- providing OCR with documentation of its compliance gap analysis; and
- reporting certain incidents to the Department for a two-year period.

Resolution Agreement with WellPoint, Inc.

The investigation by OCR followed a breach report submitted by WellPoint, Inc. (WellPoint), reporting the breach of unsecured ePHI. OCR's investigation indicated that a security weakness in an online application database left the ePHI of 612,402 individuals accessible to unauthorized individuals over the internet. The information included names, dates of birth, addresses, Social Security Numbers, telephone numbers, and health information.

On July 8, 2013, the Department reached an agreement with WellPoint to settle potential violations of the HIPAA Privacy and Security Rules. To resolve the Department's investigation, WellPoint agreed to pay $1.7 million.

Resolution Agreement with Affinity Health Plan, Inc.

Following a breach report submitted by Affinity, OCR conducted an investigation that revealed that Affinity impermissibly disclosed the ePHI of up to 344,579 individuals when it failed to properly erase photocopier hard drives prior to sending the photocopiers back to a leasing company. Additionally, OCR's investigation revealed that Affinity failed to assess and identify the potential security risks and vulnerabilities of ePHI stored on photocopier hard drives, and failed to implement policies for the disposal of photocopier hard drives containing ePHI.

On August 7, 2013, the Department reached an agreement with Affinity Health Plan, Inc. (Affinity) to settle potential violations of HIPAA. To resolve the Department's investigation, Affinity agreed to pay $1,215,780 and to take corrective action that includes:

- making best efforts to retrieve all photocopier hard drives and safeguard all such ePHI;
- conducting a comprehensive risk analysis of the ePHI security risks and vulnerabilities for all electronic equipment and systems controlled, owned, or leased by Affinity;
- developing a plan to address and mitigate any security risks and vulnerabilities found in its analysis and, if necessary, revise its present policies and procedures; and
- implementing the plan and distributing and training staff members on any revised policies and procedures.

OCR Audits of the Breach Notification Rule

Section 13411 of the HITECH Act, which became effective on February 17, 2010, authorizes and requires the Department to provide for periodic audits to ensure that covered entities and business associates comply with the HIPAA Rules. Audits, unlike complaint investigations or compliance reviews, are reviews of covered entities and business associates that are initiated not because of any particular event or incident indicating possible noncompliance on the part of the covered entity or business associate, but rather based on application of a set of objective selection criteria.

Audits present a new opportunity to examine mechanisms for compliance, identify best practices, and discover risks and vulnerabilities that may not have come to light through OCR's ongoing complaint investigations and compliance reviews. OCR will share best practices learned through the audit process and develop guidance targeted to address compliance challenges uncovered.

To implement the audit mandate, OCR piloted a program to perform 115 audits of covered entities of varying types and sizes using protocol materials to assess privacy, and security compliance. OCR engaged the services of a professional public accounting firm (KPMG LLP) to conduct performance audits, using generally accepted government auditing standards. All audits in this pilot were completed by the end of December 2012.

The OCR HIPAA pilot Audit program analyzed processes, controls, and policies of covered entities. OCR established a comprehensive audit protocol that contains the requirements to be assessed through these performance audits. The protocol covers requirements for the Breach Notification Rule, and is available at: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html.

The pilot audits looked at covered entities' compliance with specific aspects of the Breach Notification Rule:

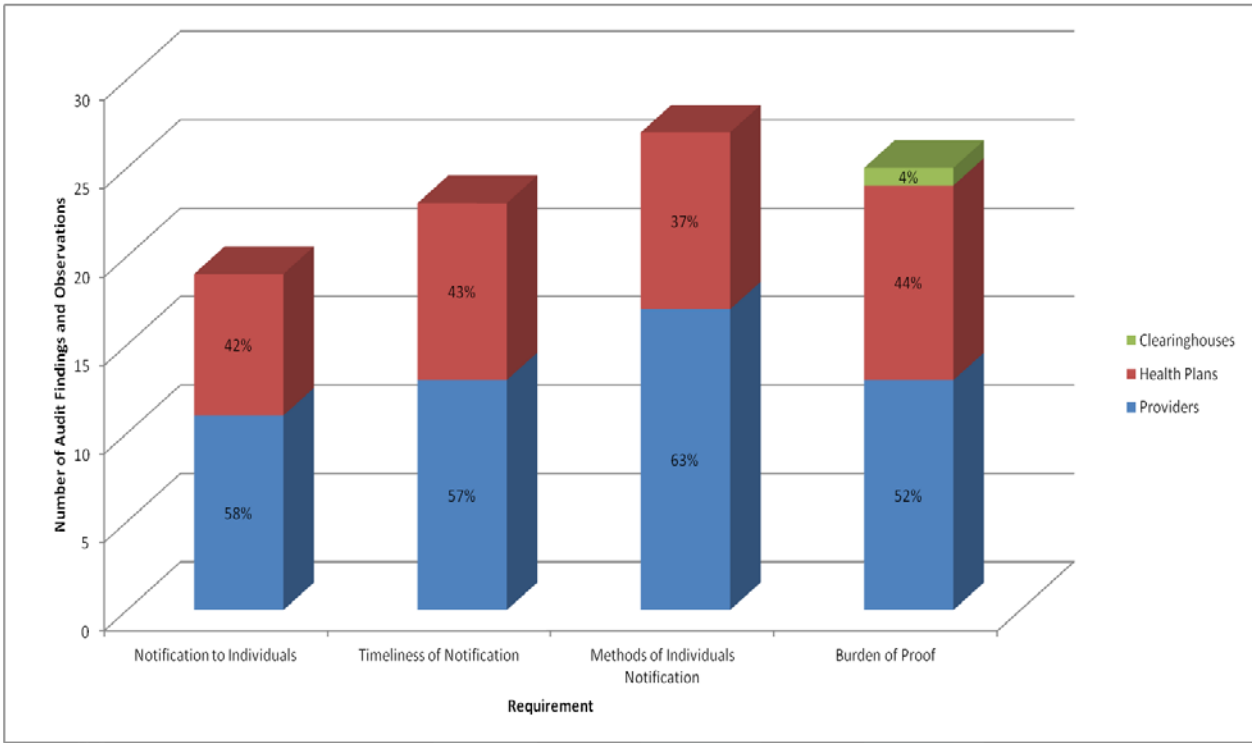
- Notification to Individuals;
- Timeliness of Notification;
- Methods of Individual Notification; and
- Burden of Proof.

The chart below represents the number of audit findings and observations by type of covered entity for each requirement of the Breach Notification Rule that was audited. In general, the most common reason covered entities provided for failing to comply with a provision of the HIPAA Rules was that they were unaware of the requirement. Other reasons included lack of application of sufficient resources, incomplete implementation, and complete disregard. As demonstrated by the chart below, of the covered entities selected for an audit, healthcare providers struggled with compliance with the audited breach requirements slightly more frequently than health plans.

There were 101 entities that were audited for the Breach Notification Rule Requirements. Of the 101 audited entities, 31 had at least 1 audit finding or observation relating to the Breach Notification Rule. The chart below represents the number of audit findings and observations by type of covered entity for each requirement of the Breach Notification Rule that was audited. In general, the audits looked at covered entities' compliance with specific aspects of the Breach Notification Rule and found findings and/or observations as follows:

- Notification to Individuals: 19 total findings/observations (11 at healthcare providers; 8 at health plans);
- Timeliness of Notification: 23 total findings/observations (13 at healthcare providers; 10 at health plans);
- Methods of Individual Notification: 27 total findings/observations (17 at healthcare providers; 10 at health plans); and
- Burden of Proof: 25 total findings/observations (13 at healthcare providers; 11 at health plans; 1 at a healthcare clearinghouse).

Audit Findings and Observations by Requirement and Type of Entity
for Breach Notification Rule Requirements



Lessons Learned

Much can be learned from the breach reports in terms of areas of vulnerability in the privacy and security of individuals' health information. Based on the breaches reported to OCR, below are a few of the areas to which covered entities should pay particular attention in their compliance efforts to help avoid some of the more common types of breaches.

- Risk Analysis and Risk Management. Ensure the organization's security risk analysis and risk management plan are thorough, having identified and addressed the potential risks and vulnerabilities to all ePHI in the environment, regardless of location or media. This includes, for example, ePHI on computer hard drives, digital copiers and other equipment with hard drives, USB drives, laptop computers, mobile phones, and other portable devices, and ePHI transmitted across networks.

- Security Evaluation. Conduct a security evaluation when there are operational changes, such as facility or office moves or renovations, that could affect the security of PHI, and ensure that appropriate physical and technical safeguards remain in place during the changes to protect the information when stored or when in transit from one location to another. In addition, conduct appropriate technical evaluations where there are technical

upgrades for software, hardware, and websites or other changes to information systems to ensure PHI will not be at risk when the changes are implemented.

- Security and Control of Portable Electronic Devices. Ensure PHI that is stored and transported on portable electronic devices is properly safeguarded, including through encryption where appropriate. Have clear policies and procedures that govern the receipt and removal of portable electronic devices and media containing PHI from a facility, as well as that provide how such devices and the information on them should be secured when off-site.

- Proper Disposal. Implement clear policies and procedures for the proper disposal of PHI in all forms. For electronic devices and equipment that store PHI, ensure the device or equipment is purged or wiped thoroughly before it is recycled, discarded, or transferred to a third party, such as a leasing agent.

- Physical Access Controls. Ensure physical safeguards are in place to limit access to facilities and workstations that maintain PHI.

- Training. Ensure employees are trained on the organization's privacy and security policies and procedures, including the appropriate uses and disclosures of PHI, and the safeguards that should be implemented to protect the information from improper uses and disclosures; and ensure employees are aware of the sanctions and other consequences for failure to follow the organization's policies and procedures.

Summary and Conclusion

For breaches occurring in 2011 and 2012, breaches involving 500 or more individuals made up 0.97 percent of reports (458 reports affecting 500 or more individuals out of 47,357 total reports), yet accounted for 97.89 percent of the 15,005,660 individuals who were affected by a breach of their PHI. Similarly, in 2009 and 2010, breaches affecting 500 or more individuals made up less than one percent of reports, but accounted for more than 99 percent of the individuals affected by a breach of their PHI. In 2011, theft and loss of PHI affected the largest numbers of individuals. In 2012, theft and hacking/IT incidents affected the largest numbers of individuals. Of all of the categories of causes of breaches, theft continues to be one of the top causes that affects the most individuals.

The breach notification requirements are achieving their twin objectives of increasing public transparency in cases of breach and increasing accountability of covered entities and business associates. The reports submitted to OCR indicate that millions of affected individuals are receiving notifications of breaches. 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, name of business associate, if applicable, 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 enforcement cases, including cases stemming from a breach report, 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, as well as into a number of breaches involving fewer than 500 individuals. For breaches occurring through the end of 2012, OCR had opened investigations into over 700 breaches, including the 458 breaches affecting 500 or more individuals that occurred in 2011 and 2012. OCR has closed some of these cases after investigation when OCR determined 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 addition, in seven cases resulting from a breach report, the Department has entered into resolution agreements/corrective action plans totaling more than $8 million in settlements. As of the date of this report, OCR has over 500 open investigations that were opened as the result of a breach report. In these remaining open investigations, 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.