Annual Report to Congress on Breaches of Unsecured Protected Health Information

For Calendar Years 2013 and 2014

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 2013 and 2014.[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. All previous Reports to Congress are available on OCR's website: http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/reports-congress/index.html

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.

[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.

- **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 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, 2013, and December 31, 2014, 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. Additional information on OCR's compliance and enforcement efforts in other areas may be found in OCR's Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance for Calendar Years 2013 and 2014. 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, in addition to requiring covered entities and business associates to take corrective action in hundreds of cases, for 2013 and 2014, the Department has entered into fifteen resolution agreements/corrective action plans totaling more than $10 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 294 reports of these larger breaches that occurred in calendar year 2013,[3] which affected a total of approximately 8,170,622 individuals.[4] For breaches occurring in calendar year 2014, OCR received 277 reports of these larger breaches, which affected a total of approximately 21,345,240 individuals. Cumulatively, from September 23, 2009, to December 31, 2014, OCR received 1187 reports of large breaches affecting a total of approximately 41.2 million individuals.

The 2009/2010 Annual Report to Congress[5] 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 after, 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 2011-2014 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 2011-2014 charts. For the charts covering only the years 2013 and 2014, all six categories of causes of breaches are included. [6]

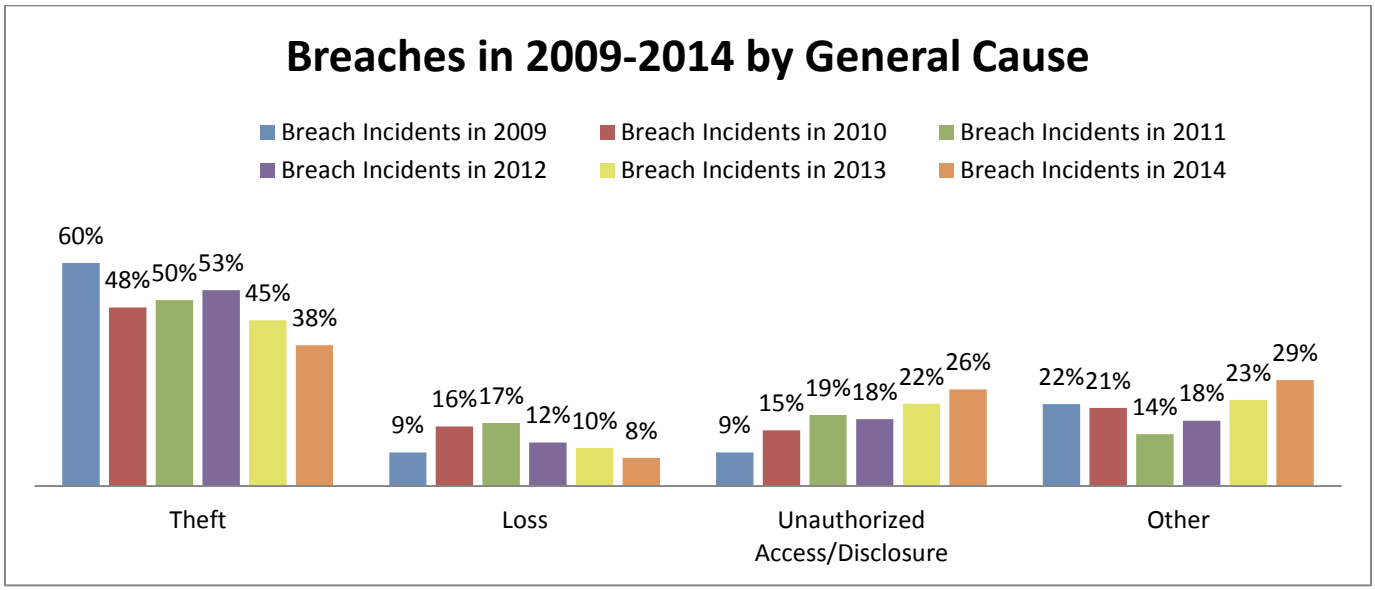
[3] The Department receives some reports where the breach occurred over the period of several years. For the purposes of this report, breach incidents spanning multiple years are included with the data for the last year in which the breach occurred, e.g., a breach incident that continued from 2013 to 2014 would be reported with the 2014 numbers.

[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.

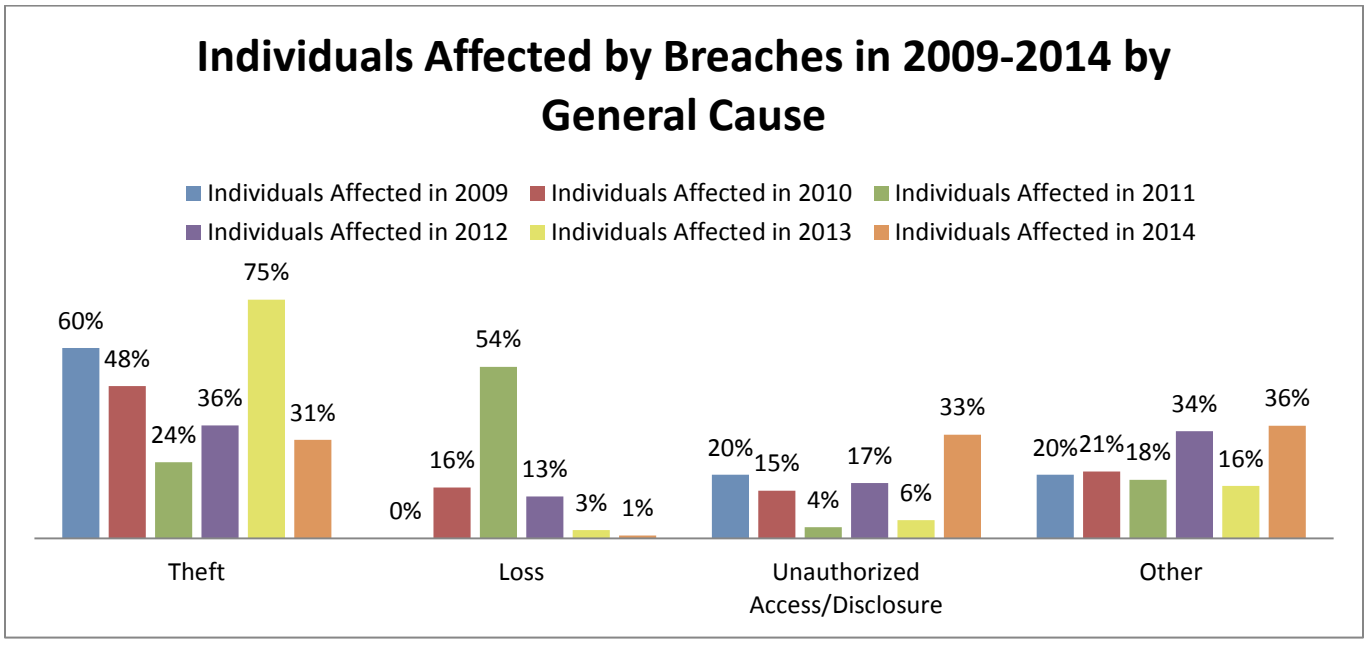
[5] See the Annual Report to Congress on Breaches of Unsecured Protected Health Information For Calendar Years 2009 and 2010, available at http://www.hhs.gov/hipaa/for-professionals/breach-notification/reports-congress/index.html.

[6] 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 2009-2014 categorized by four general causes of breaches.[7]

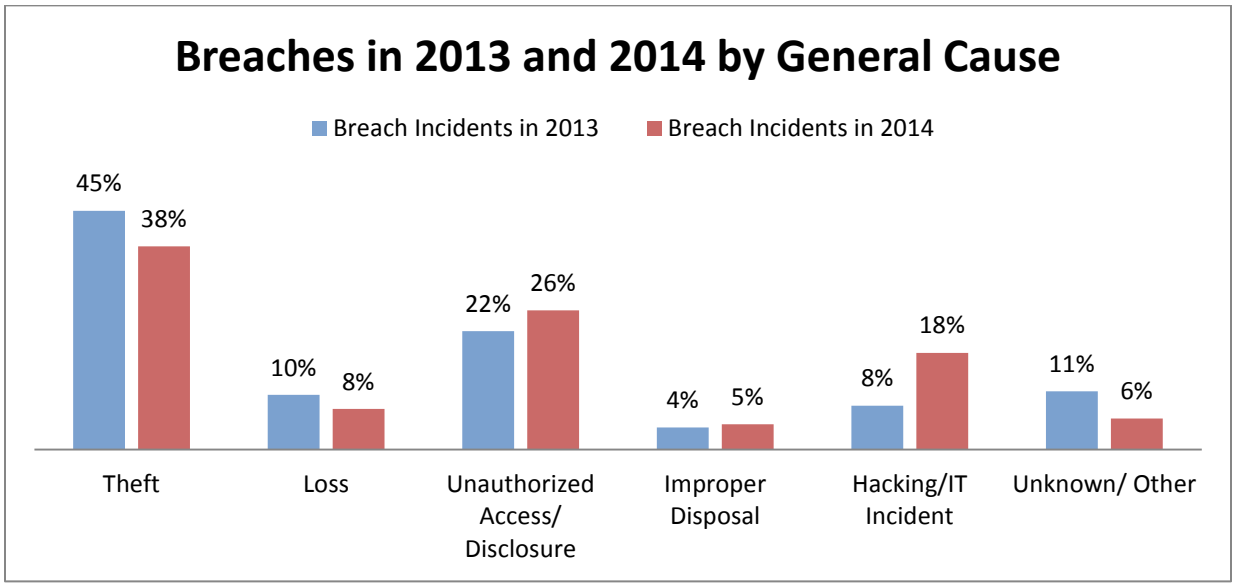


The following chart shows the percentage of individuals affected by breaches in 2009 –2014 by four general causes of breaches.

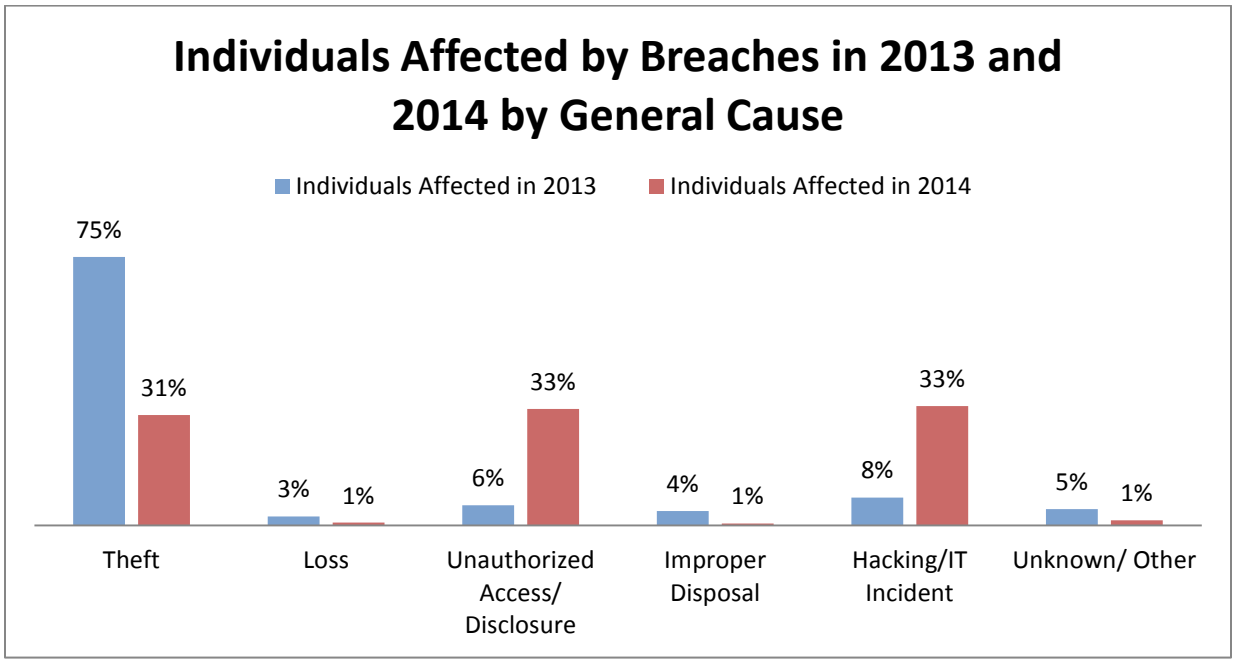


[7] All percentages shown in the charts in this report are rounded to the nearest whole number and, therefore, may not add up to 100% in all cases.

The following chart shows the percentage of breaches in 2013 and 2014 categorized by six general causes of breaches.

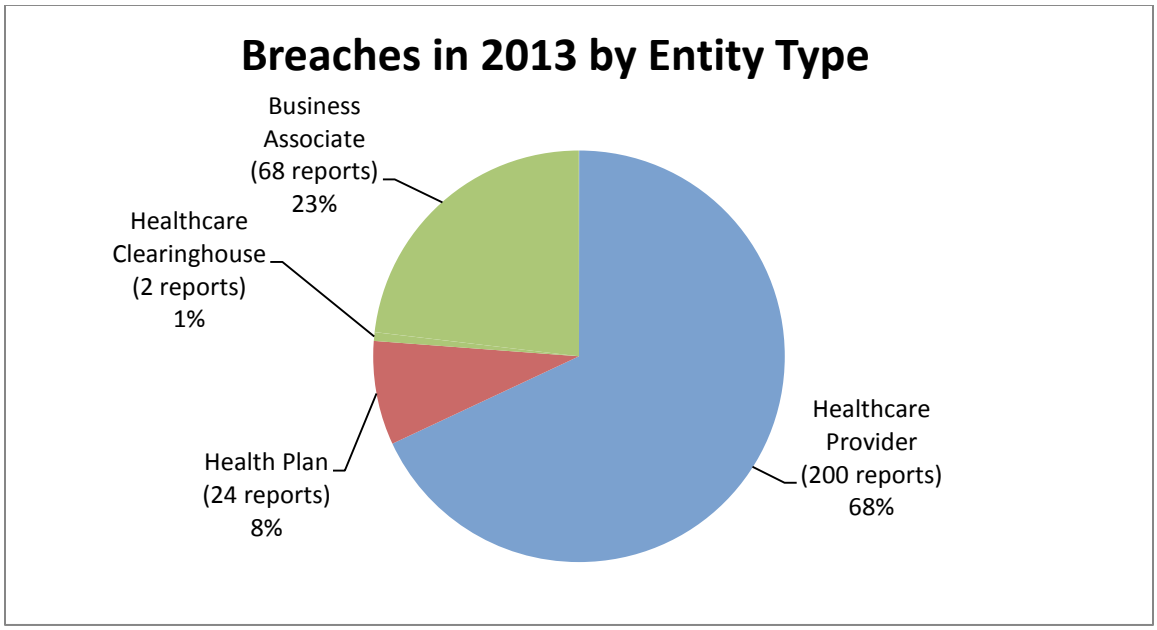


The following chart shows the percentage of individuals affected by breaches in 2013 and 2014 by six general causes of breaches.

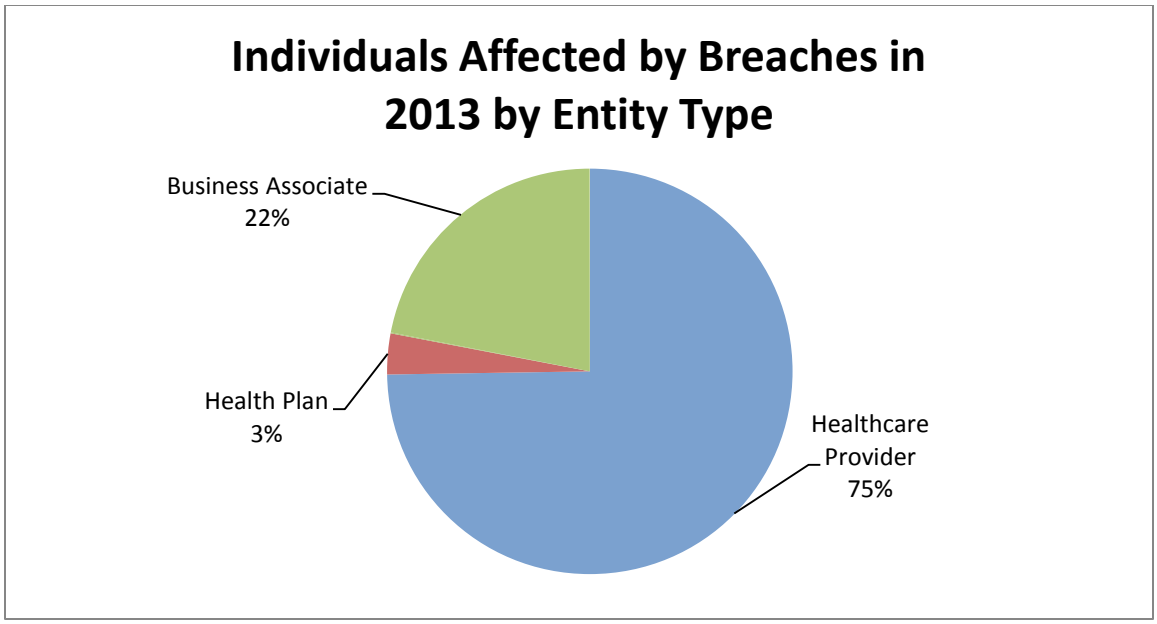


Breaches in 2013 Affecting 500 or More Individuals

For the 294 breaches in 2013 affecting 500 or more individuals, OCR received 200 reports, or sixty-eight percent, of breaches at healthcare providers (affecting a total of 6,107,830 individuals, or seventy five percent); 24 reports, or eight percent, of breaches at health plans (affecting a total of 265,684 individuals, or three percent); two reports, or one percent, of breaches at clearinghouses (affecting a total of 6,504[8] individuals); and 68 reports, or twenty-three percent, of breaches at business associates (affecting a total of 1,790,604 individuals, or twenty-two percent).

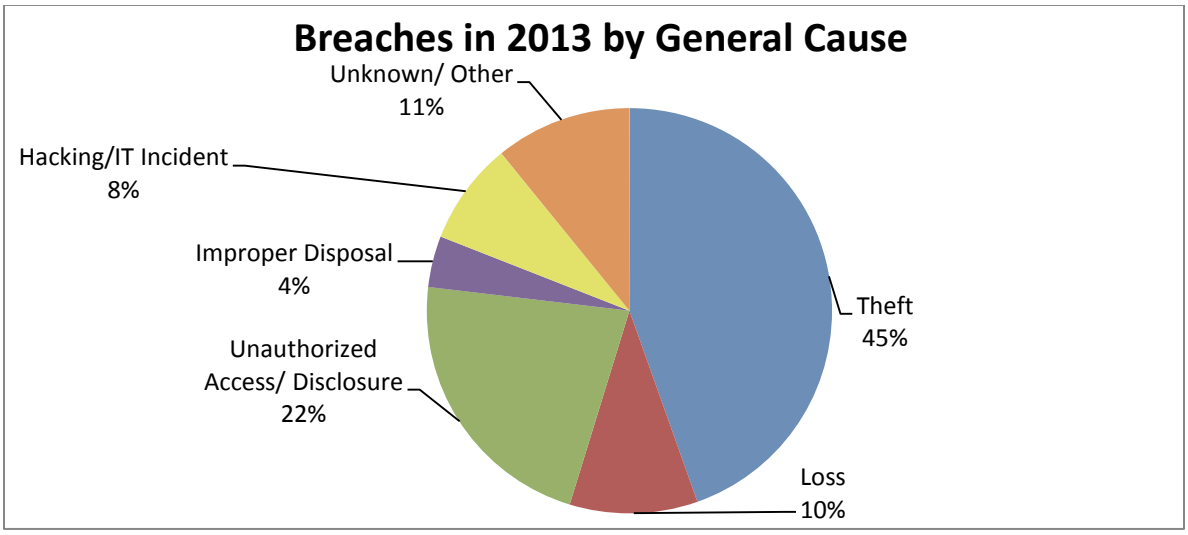


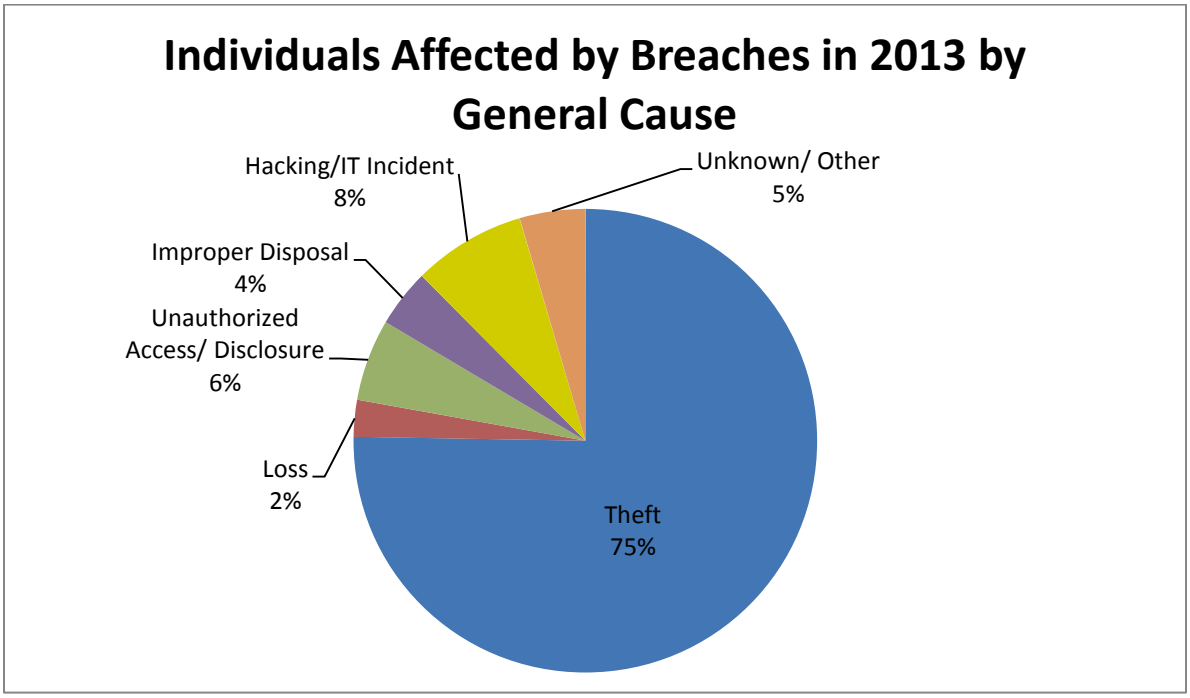
[8] In instances in which the percentage is less than one percent, and is, therefore, statistically insignificant, the percentage is not reported.



The 294 reports for breaches occurring in 2013 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 (131 reports, or forty-five percent, affecting 6,149,295 individuals, or seventy-five percent);
(2) unauthorized access or disclosure of records containing PHI (65 reports, or twenty-two percent, affecting 465,060 individuals, or six percent);
(3) unknown/other causes of breaches of PHI (32 reports, or eleven percent, affecting 374,104 individuals, or five percent);
(4) loss of electronic media or paper records containing PHI (30 reports, or ten percent, affecting 210,245 individuals, or three percent);
(5) hacking/IT incident of electronic equipment or a network server (24 reports, or eight percent, affecting 642,318 individuals, or eight percent); and
(6) improper disposal of PHI (12 reports, or four percent, affecting 329,600 individuals, or four percent).

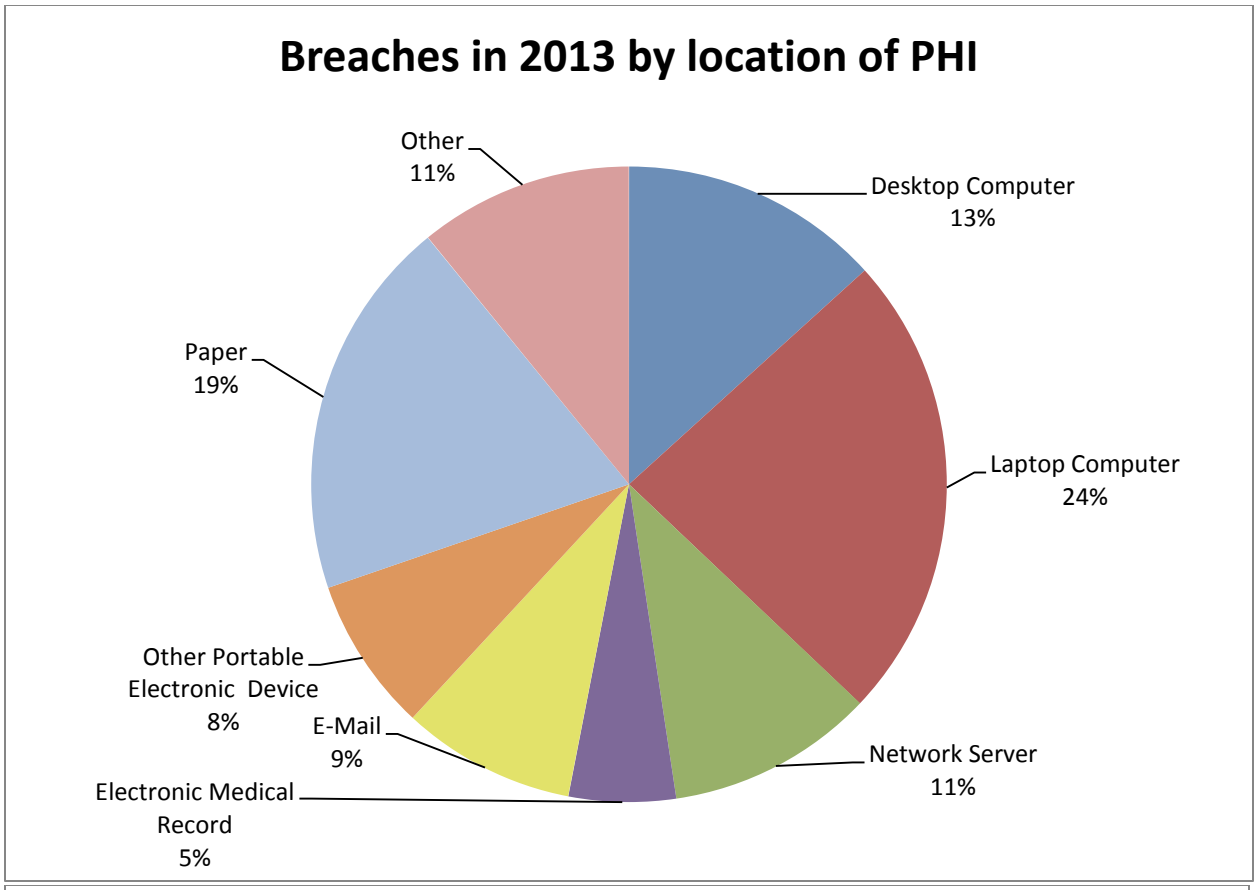


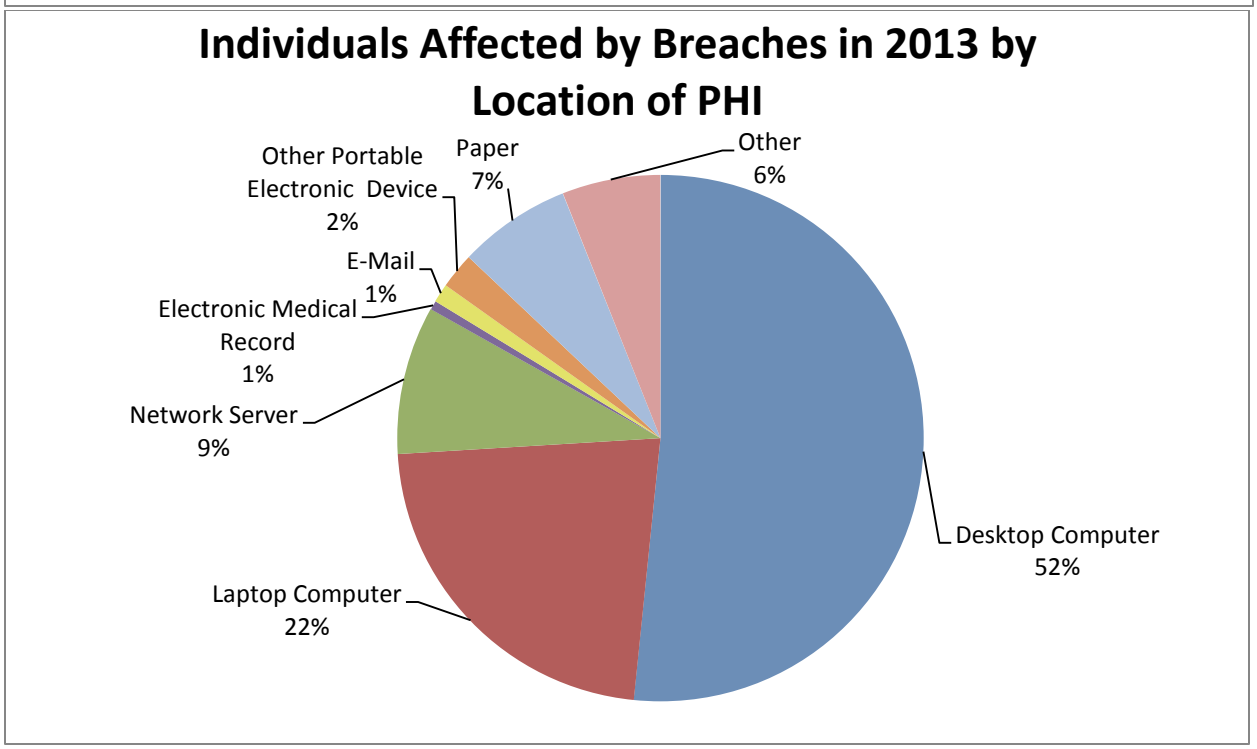


The 294 reports for breaches occurring in 2013 described the following locations of the PHI (in order of frequency):[9]

(1) laptop computer (70 reports, or twenty-four percent, affecting 1,831,653 individuals, or twenty-two percent);
(2) paper (57 reports, or nineteen percent, affecting 565,004 individuals, or seven percent);
(3) desktop computer (39 reports, or thirteen percent, affecting 4,217,848 individuals, or fifty-two percent);
(4) other (32 reports, or eleven percent, affecting 493,542 individuals, or six percent);
(5) network server (31 reports, or eleven percent, affecting 743,569 individuals, or nine percent);
(6) e-mail (26 reports, or nine percent, affecting 93,995 individuals, or one percent);
(7) other portable electronic device (23 reports, or eight percent, affecting 179,557 individuals, or two percent); and
(8) electronic medical record (16 reports, or five percent, affecting 45,454 individuals, or one percent).

[9]Despite instructions on OCR's website regarding how to file breach reports, some covered entities and business associates 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.


Breaches in 2013 by location of PHI
Other
11%
Desktop Computer
13%
Paper
19%
Laptop Computer
24%
Other Portable
Electronic Device
8%
E-Mail
9%
Network Server
11%
Electronic Medical
Record
5%


Individuals Affected by Breaches in 2013 by
Location of PHI
Other Portable
Electronic Device
2%
Paper
7%
Other
6%
E-Mail
1%
Electronic Medical
Record
1%
Network Server
9%
Desktop Computer
52%
Laptop Computer
22%

Largest breaches in 2013 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 2013 was the result of a burglary at the office of a covered entity that affected approximately 4 million individuals. Four unencrypted computers were stolen that contained individuals' PHI. 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 hacking/IT incident in 2013, affecting 405,000 individuals, involved hackers gaining access to a server on the covered entity's computer system through the unauthorized access to various records by current and former employees that was used to exploit their computer system. Other hacking/IT incidents involved the use of malware to gain access to computer systems, employees opening e-mail attachments that contain viruses, and the posting of PHI to public websites.

The largest improper disposal breach for 2013 involved the disposal of microfiche films affecting approximately 277,014 individuals. In this case, the business associate of the covered entity did not properly dispose of films which contained PHI. Members of the community began finding films in multiple public parks and other public areas and notified the covered entity. Most of the improper disposal cases involving paper records were the result of employees improperly disposing of documents containing PHI in regular containers other than authorized shredding containers.

The largest breach reported as having an "other" cause in 2013 affected 187,533 individuals and involved a business associate who comingled documents containing PHI and mailed them to the wrong recipients. Other breaches in 2013 involving "other" causes were the result of misdirected mailings.

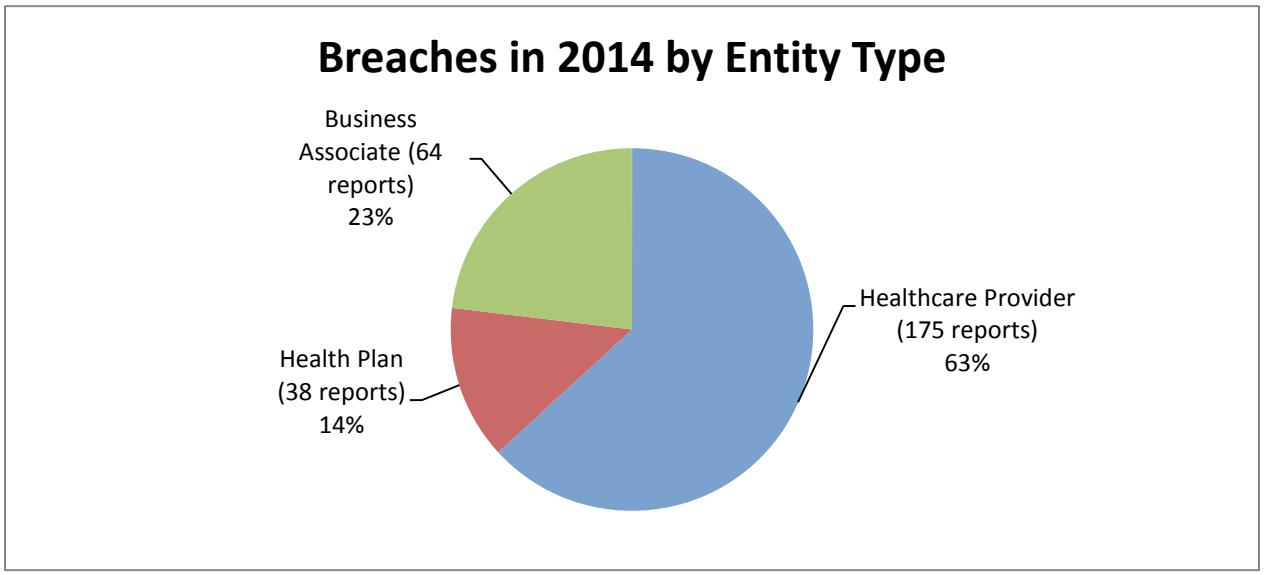
The largest breach in 2013 involving the unauthorized disclosure, as reported by the entity, of PHI occurred when pamphlets that were mailed to individuals with the envelope displaying all or part of the individuals' insurance claim numbers. This breach affected 70,189 individuals. Other reports of unauthorized access or disclosure of PHI involved mailing errors, as well as employees viewing or removing PHI for purposes beyond the scope of their duties.

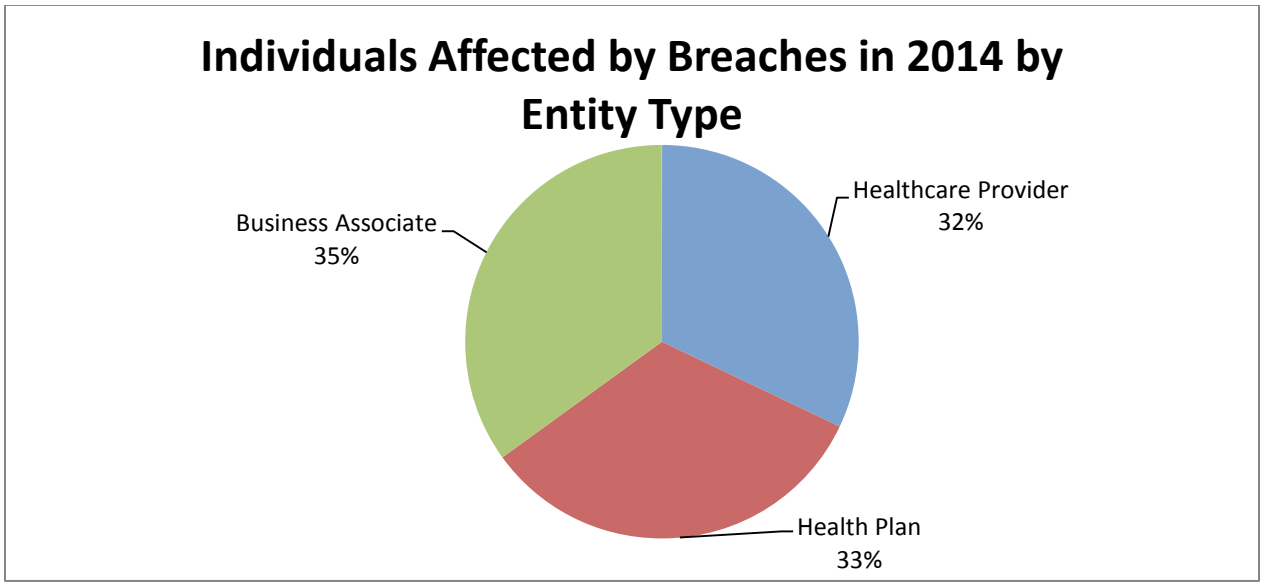
The largest breach as a result of a loss for 2013 involved an unencrypted flash drive that the covered entity discovered was missing from its office. The breach affected 49,000 individuals. Other incidents reported as a loss of PHI involved a variety of paper and electronic media that could not be located or were lost in transit.

The largest breach reported with an unknown cause in 2013 affected 953 individuals. It involved a notebook containing PHI that could not be located.

Breaches in 2014 Affecting 500 or More Individuals

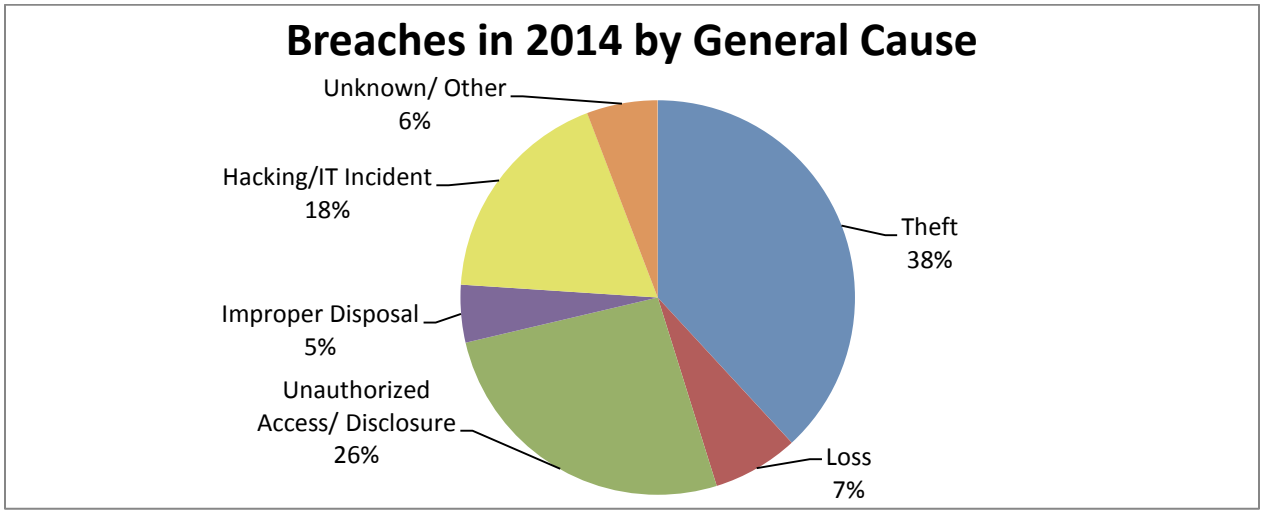
For breaches affecting 500 or more individuals in 2014, OCR received 175 reports, or sixty-three percent, of breaches at healthcare providers (affecting a total of 6,851,614, or thirty-two percent, of individuals); 64 reports, or twenty-three percent, of breaches at business associates (affecting a total of 7,470,192, or thirty-five percent, of individuals); and 38 reports, or fourteen percent, of breaches at health plans (affecting a total of 7,023,434, or thirty-three percent, of individuals.

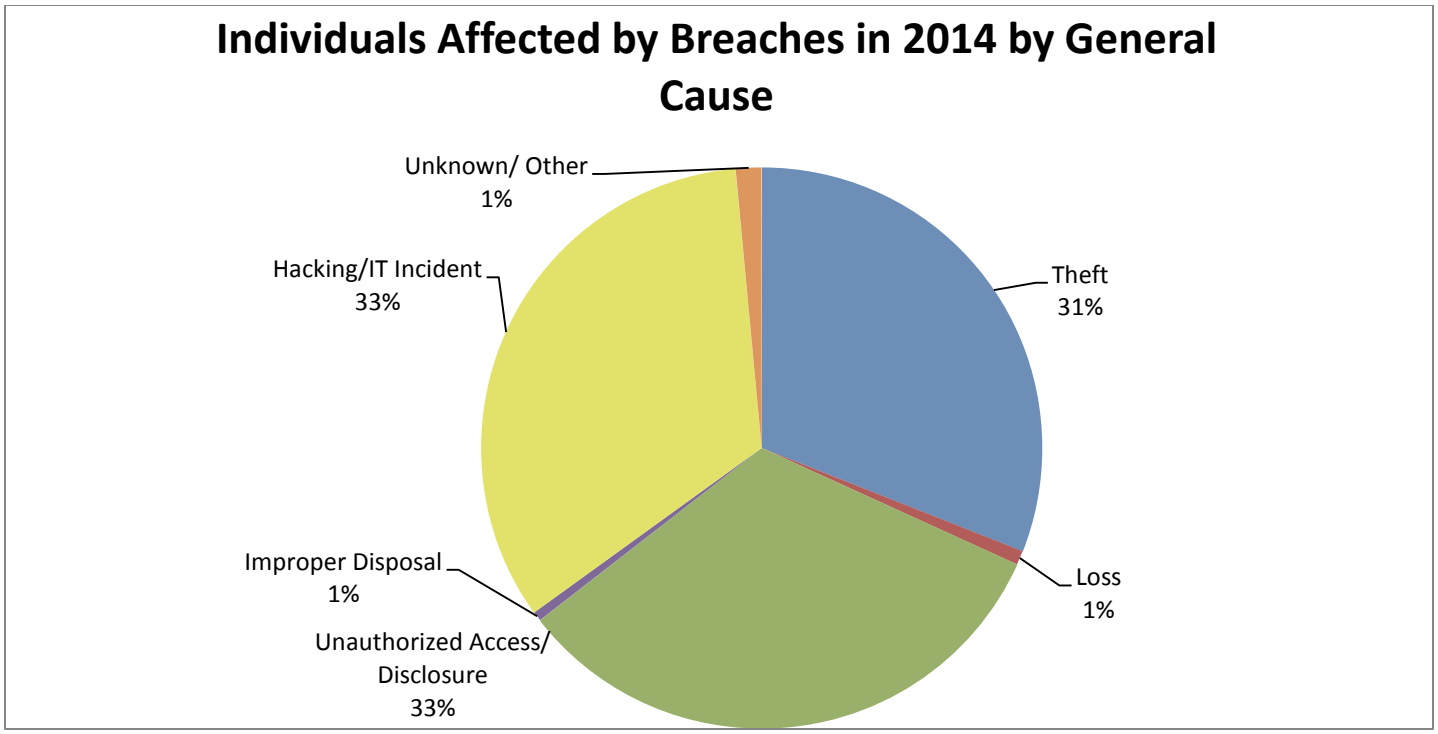




The 277 reports submitted to OCR for breaches occurring in 2014 can be categorized by six general causes of incidents as follows (in order of frequency):

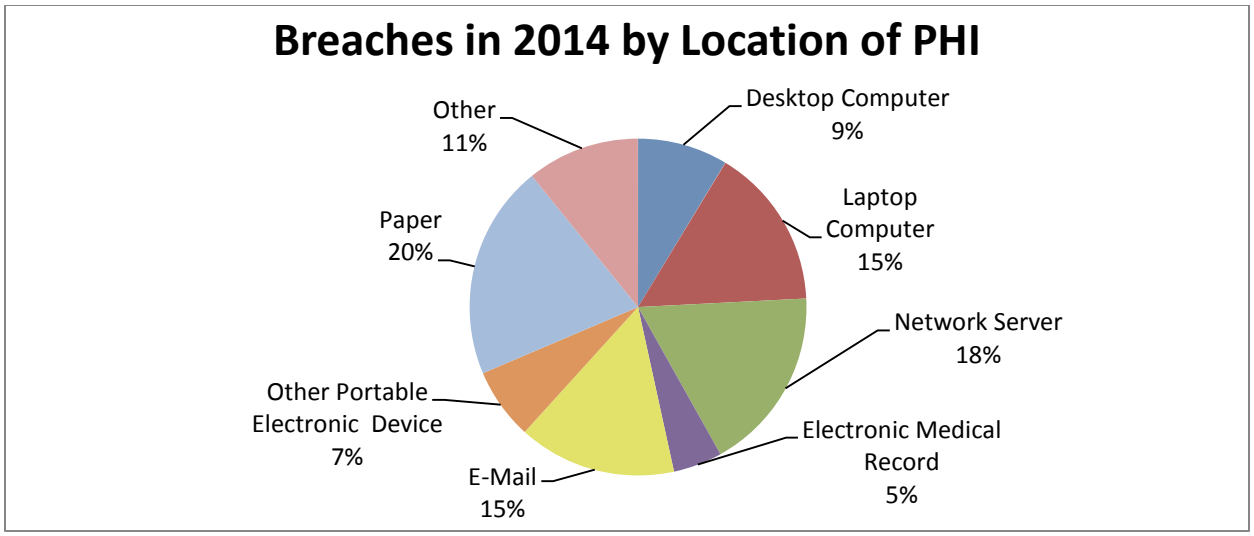
(1) theft of electronic equipment/portable devices or paper containing PHI (105 reports, or thirty-eight percent, affecting 6,615,929 individuals, or thirty-one percent);
(2) unauthorized access or disclosure of records containing PHI (72 reports, or twenty-six percent, affecting 6,976,208, or thirty-three percent, of individuals);
(3) hacking/IT incident of electronic equipment or a network server (50 reports, or eighteen percent, affecting 7,144,137 individuals, or thirty-three percent);
(4) loss of electronic media or paper records containing PHI (21 reports, or seven percent, affecting 174,074 individuals, or one percent);
(5) other causes of breaches of PHI (16 reports, or six percent, affecting 318,296 individuals, or one percent); and
(6) improper disposal of PHI (13 reports, or five percent, affecting 116,596 individuals, or one percent).

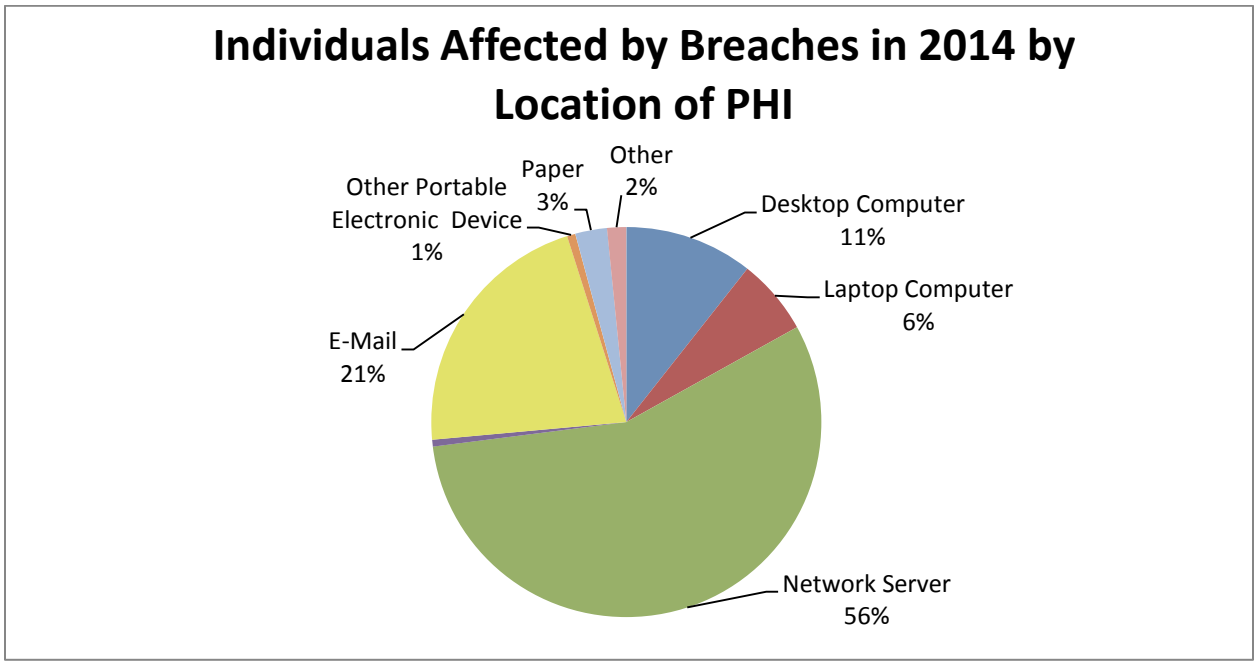




The 277 reports submitted to OCR for breaches occurring in 2014 described the following locations of the PHI (in order of frequency):

(1) paper (57 reports, or twenty percent, affecting 563,352 individuals, or three percent);
(2) network server (49 reports, or eighteen percent, affecting 11,954,442 individuals, or fifty-six percent);
(3) laptop computer (43 reports, or fifteen percent, affecting 1,342,271 individuals, or six percent);
(4) e-mail (42 reports, or fifteen percent, affecting 4,591,889 individuals, or twenty-one percent);
(5) other (30 reports, or eleven percent, affecting 336,683 individuals, or two percent);
(6) desktop computer (24 reports, or nine percent, affecting 2,267,928 individuals, or eleven percent);
(7) other portable electronic device (19 reports, or seven percent, affecting 147,261 individuals, or one percent); and
(8) electronic medical record (13 reports, or five percent, affecting 121,414 individuals).





Largest breaches in 2014 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 2014 resulting from theft involved six desktop computers that were stolen from a business associate's office during a burglary. This incident affected 168,490 individuals. Other reports of theft of PHI reported for 2014 involved thefts of laptops and other portable electronic devices from employees' vehicles, medical official offices, and healthcare facilities.

The two largest breaches in 2014 resulting from hacking/IT incidents were also the largest breaches in 2014. Both incidents involved cyber-attacks of hospitals' computer networks which compromised the PHI of approximately 4.5 million individuals in both incidents. Other hacking/IT incidents involved covered entities that discovered viruses or malware, or unidentified, unauthorized persons obtaining access to systems.

The largest breach in 2014 involving the unauthorized access or disclosure of PHI affected two million individuals. In this case, a business associate did not safeguard PHI upon the termination of contractual services. Other incidents of unauthorized access or disclosure involved employees impermissibly accessing records outside the scope of their job responsibilities, misdirected communications, and PHI accessible via the internet.

The largest breach in 2014 reported as having an "other" cause involved a covered entity that due to human error mailed PHI to the wrong recipients over a three-month period. This breach affected approximately 160,000 individuals. This type of breach was routinely reported throughout the year by various covered entities and business associates.

The largest reported incident in 2014 involving improper disposal resulted from the improper disposal of x-rays. An investigation by a business associate revealed that several employees were responsible for taking x-rays and melting them down to recover the silver they contain. This breach affected 49,714 individuals. 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 2014 involved a missing server from a physician's office. This incident affected approximately 47,683 individuals. Other incidents involving the loss of PHI in 2014 involved missing unencrypted backup tapes, unencrypted USB drives, and paper records from a healthcare provider's office.

Remedial Action Reported

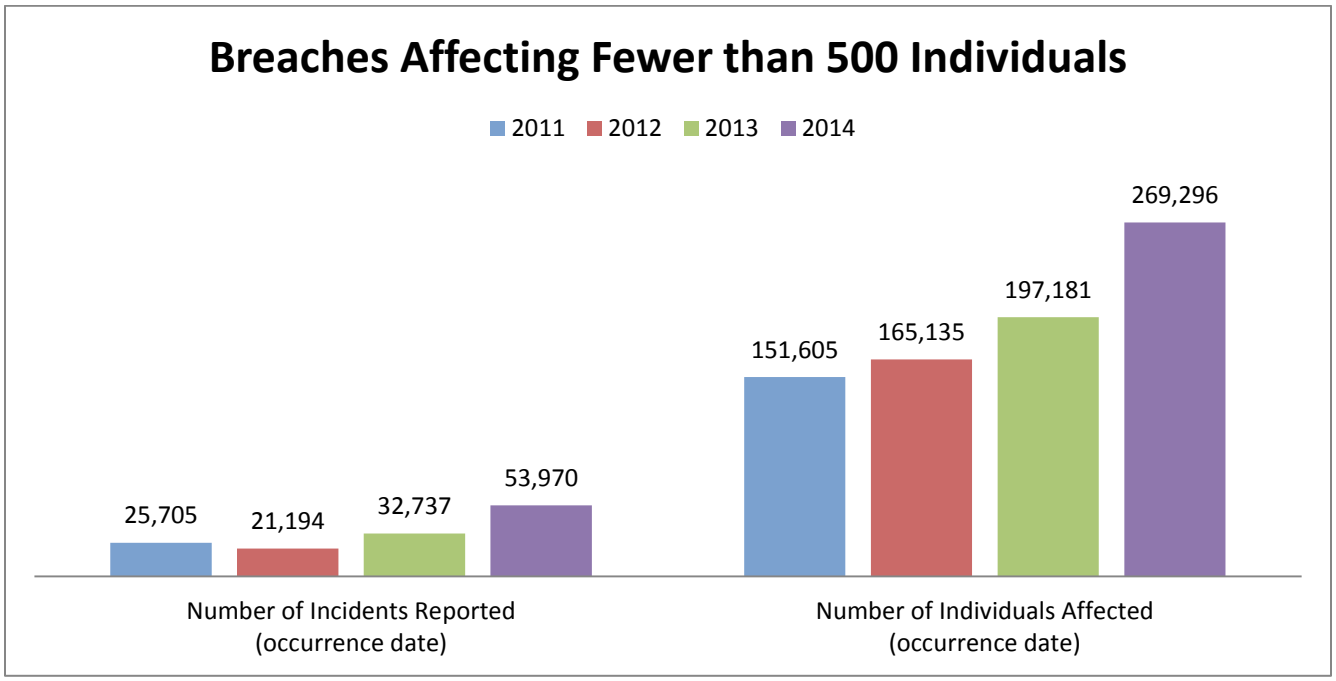
For breaches affecting 500 or more individuals that occurred in 2013 and 2014, in addition to providing the required notifications, covered entities most commonly reported taking one or more of the following steps to mitigate the potential consequences of the breaches and prevent future breaches:

- 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 2013, notification to OCR was required no later than March 1, 2014. For breaches discovered during 2014, notification to OCR was required no later than March 1, 2015.

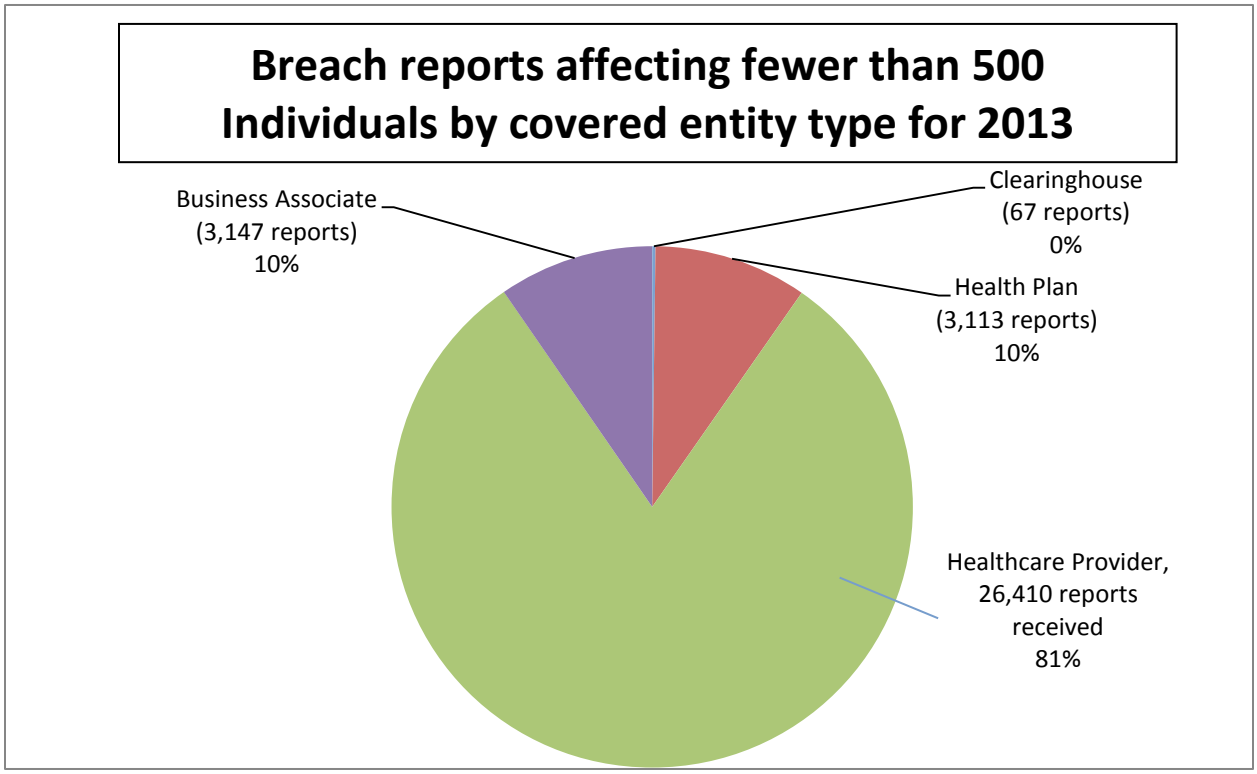


This chart represents the number of incidents reported to OCR and the number of individuals affected by those incidents, by the year the breach occurred for the past four years.

Breaches involving fewer than 500 individuals for 2013

OCR received approximately 32,737 reports of smaller breaches that occurred between January 1, 2013, and December 31, 2013. These smaller breaches affected approximately 197,181 individuals. Of these reports of smaller breaches, 3,113, or ten percent, were reported by health plans (affecting 16,379 individuals, or eight percent); 26,410, or eighty-one percent,

were reported by healthcare providers (affecting 140,211 individuals, or seventy-one percent); 67 were reported by healthcare clearinghouses (affecting 266 individuals); [10] and 3147, or ten percent, were reported by business associates (affecting 40,325, or twenty percent).



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

(1) unauthorized access or disclosure (26,291 reports, or eighty percent, affecting 114,522 individuals, or fifty-eight percent);
(2) unknown/other (3,974 reports, or twelve percent, affecting 55,190 individuals, or twenty-eight percent);
(3) theft (1,166 reports, or four percent, affecting 17,328 individuals, or nine percent);
(4) loss (1032 reports, or three percent, affecting 5,285 individuals, or three percent);
(5) improper disposal (199 reports, or one percent, affecting 3,755 individuals, or two percent); and
(6) hacking/IT incident (75 reports affecting 1,101 individuals, or one percent).

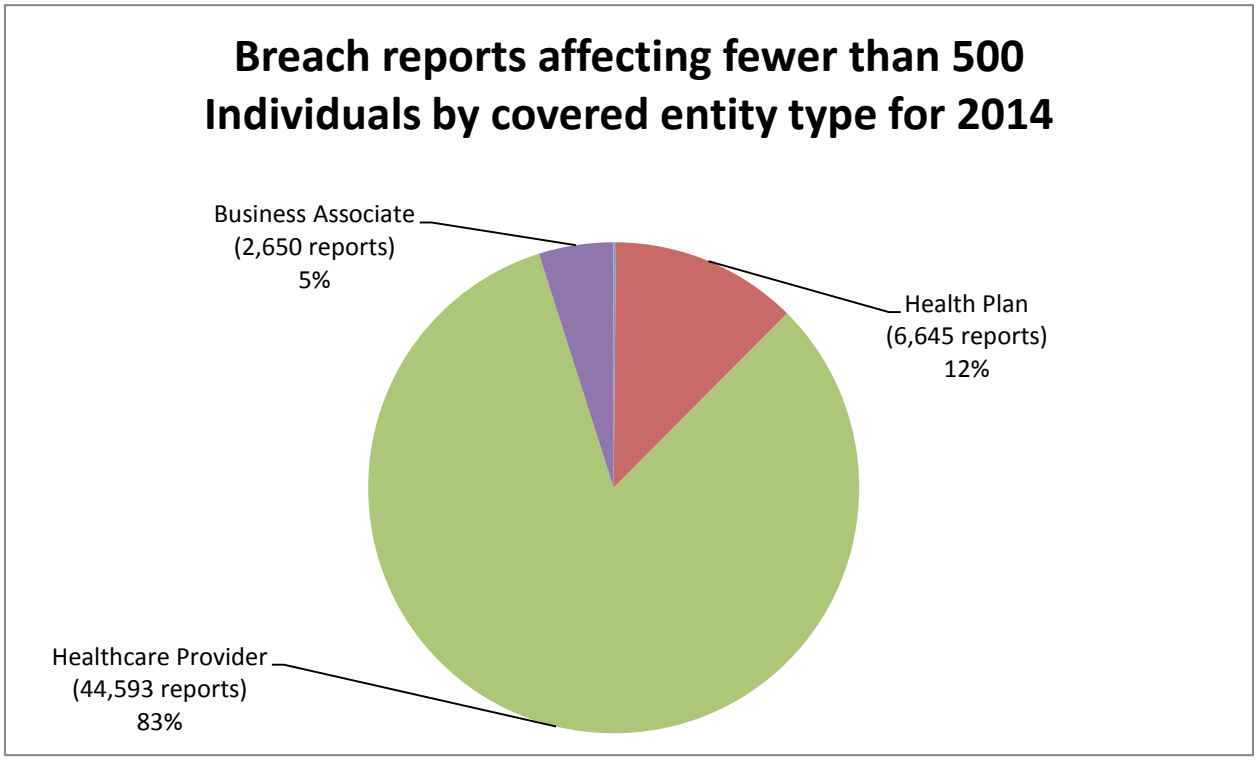
Of these reports, 20,835 reports, or sixty-four percent, involved paper records (affecting 84,729 individuals, or forty-three percent); 2,579 reports, or eight percent, involved an electronic medical record (affecting 11,709 individuals, or six percent); 1,025 reports, or three percent, involved desktop computers (affecting 9016 individuals, or five percent); 909 reports, or three

[10] In instances in which the percentage is less than one percent, and is, therefore, statistically insignificant, the percentage is not reported.

percent, involved e-mail (affecting 16,428 individuals, or eight percent); 456 reports, or one percent, involved portable electronic devices (affecting 9,368 individuals, or five percent); 242 reports, or one percent, involved laptops (affecting 17,970 individuals, or nine percent); 328 reports, or one percent, involved network servers (affecting 7,147 individuals, or four percent); and 6,363 reports, or nineteen percent, (affecting 40,814 individuals, or twenty-one percent) did not identify the location of the data that was breached.

Breaches involving fewer than 500 individuals for 2014

OCR received approximately 53,970 reports of smaller breaches that occurred between January 1, 2014, and December 31, 2014. These smaller breaches affected approximately 269,296 individuals. Of these reports of smaller breaches, 6,645, or twelve percent, were reported by health plans (affecting 76,061 individuals, or twenty-eight percent); 44,593, or eighty-three percent, were reported by health care providers (affecting 164,708 individuals, or sixty-one percent); 82 were reported by health care clearinghouses (affecting 82 individuals); and 2,650, or five percent, were reported by business associates (affecting 28,445 individuals, or eleven percent).



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

(1) unauthorized access or disclosure (47,725 reports, or eighty-eight percent, affecting 214,185 individuals, or eighty percent);
(2) unknown/other (2,484 reports, or four percent, affecting 2,720 individuals, or one percent);

(3) loss (1,765 reports, or three percent, affecting 17,563 individuals, or seven percent);
(4) theft (1,434 reports, or three percent, affecting 24,269 individuals, or nine percent);
(5) improper disposal (283 reports, or one percent, affecting 1,014 individuals); and
(6) hacking/IT incident (279 reports, or one percent, affecting 9,545 individuals, or four percent).

Of these reports, 35,418 reports, or sixty-six percent, involved paper records (affecting 134,062 individuals, or fifty percent); 4,240 reports, or eight percent, involved an electronic medical record (affecting 20,038 individuals, or seven percent); 1,607 reports, or three percent, involved e-mail (affecting 24,442 individuals, or nine percent); 879 reports, or two percent, involved desktop computers (affecting 10,875 individuals, or four percent); 621 reports, or one percent, involved portable electronic devices (affecting 13,623 individuals, or five percent); 579 reports, or one percent, involved network servers (affecting 11,384 individuals, or four percent); 314 reports, or one percent, involved laptops (affecting 21,864 individuals, or eight percent); and 10,312 reports, or nineteen percent, did not identify the location of the data that was breached (affecting 33,008 individuals, or twelve percent).

Details on Breaches involving fewer than 500 individuals for 2013 and 2014

Incidents reported for 2013 and 2014 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 571 breaches affecting 500 or more individuals that occurred in 2013 and 2014. Additional information on OCR's work with regard to breaches may be found in OCR's Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance for calendar years 2013 and 2014. OCR has also opened a number of investigations into breaches affecting fewer than 500 individuals. 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. Additional information on OCR's compliance and enforcement efforts in other areas may be found in OCR's Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance for Calendar Years 2013 and 2014.

Enforcement Actions

For 2013 and 2014, OCR has entered into resolution agreements with ten covered entities as the result of investigations opened in response to breach reports submitted to OCR for breaches that occurred through the end of 2014. Under these resolution agreements, covered entities agreed to pay more than $10 million to the government. Over 2.4 million individuals were affected by the breaches that led to these investigations. Eight of these cases, including two stemming from a breach incident affecting fewer 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. Cases from 2013 and 2014 are discussed in greater detail below.

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.

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, which is a single legal entity and covered entity whose business activities include both covered and non-covered functions, and that designates health care components as permitted by the HIPAA Privacy Rule;

- 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 report submitted by WellPoint, Inc. (WellPoint) regarding 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.

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.

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.

Resolution Agreement with Adult & Pediatric Dermatology of Massachusetts

Adult & Pediatric Dermatology, P.C., of Concord, Mass., (APDerm) agreed to pay $150,000 to settle potential violations of the HIPAA Privacy, Security, and Breach Notification Rules. APDerm is a private practice that delivers dermatology services in four locations in Massachusetts and two in New Hampshire. This case was the first settlement with a covered entity for not having policies and procedures in place to address the HIPAA Breach Notification Rule.

OCR opened an investigation of APDerm upon receiving a report that an unencrypted thumb drive containing the electronic protected health information (ePHI) of approximately 2,200 individuals was stolen from a vehicle of one its staff members. The thumb drive was never recovered. The investigation revealed that APDerm had not conducted an accurate and thorough analysis of the potential risks and vulnerabilities to the confidentiality of ePHI as part of its security management process. Further, APDerm did not fully comply with requirements of the Breach Notification Rule to have in place written policies and procedures and train workforce members.

In addition to a $150,000 resolution amount, the settlement includes a corrective action plan requiring APDerm to:

- develop a risk analysis and risk management plan to address and mitigate any security risks and vulnerabilities;
- provide an implementation report to OCR.

Resolution Agreement with Skagit County Government

Skagit County, Washington, agreed to settle potential violations of the HIPAA Privacy, Security, and Breach Notification Rules. Skagit County agreed to a $215,000 monetary settlement and to work closely with the OCR to correct deficiencies in its HIPAA compliance program. Skagit County is located in Northwest Washington, and is home to approximately 118,000 residents. The Skagit County Public Health Department provides essential services to many individuals who would otherwise not be able to afford health care.

OCR opened an investigation of Skagit County upon receiving a breach report that money receipts with electronic protected health information (ePHI) of seven individuals were accessed by unknown parties after the ePHI had been inadvertently moved to a publicly accessible server maintained by the County. OCR's investigation revealed a broader exposure of protected health information involved in the incident, which included the ePHI of 1,581 individuals. Many of the accessible files involved sensitive information, including protected health information concerning the testing and treatment of infectious diseases. OCR's investigation further uncovered general and widespread non-compliance by Skagit County with the HIPAA Privacy, Security, and Breach Notification Rules.

Skagit County continues to cooperate with OCR through a corrective action plan to ensure it has in place:

- substitute breach notifications for all affected individuals; written policies and procedures;
- documentation requirements;
- training; and
- providing regular status reports to OCR.

Resolution Agreement with QCA Health Plan

QCA Health Plan paid OCR $250,000 to resolve potential violations of the HIPAA Privacy and Security Rules. This enforcement action was publicized with the action below against Concentra Health Services to highlight ongoing industry issues with unencrypted laptop computers and other mobile devices.

OCR received a breach notice from QCA Health Plan, Inc. of Arkansas reporting that an unencrypted laptop computer containing the ePHI of 148 individuals was stolen from a workforce member's car. While QCA encrypted their devices following discovery of the breach, OCR's investigation revealed that QCA failed to comply with multiple requirements of the HIPAA Privacy and Security Rules, beginning from the compliance date of the Security Rule in April 2005 and ending in June 2012. QCA agreed to a $250,000 monetary settlement and a corrective action plan that includes:

- an updated risk analysis;
- a corresponding risk management plan that includes specific security measures to reduce the risks to and vulnerabilities of its ePHI;
- retraining of its workforce; and
- documenting its ongoing compliance efforts.

Resolution Agreement with Concentra Health Services

Concentra Health Services paid the OCR $1,725,220 to resolve potential violations of the HIPAA Privacy and Security Rules. This major enforcement action underscores the significant risk to the security of patient information posed by unencrypted laptop computers and other mobile devices.

OCR opened a compliance review of Concentra Health Services (Concentra) upon receiving a breach report that an unencrypted laptop was stolen from one of its facilities, the Springfield Missouri Physical Therapy Center. OCR's investigation revealed that Concentra had previously recognized in multiple risk analyses that a lack of encryption on its laptops, desktop computers, medical equipment, tablets and other devices containing electronic protected health information (ePHI) was a critical risk. While steps were taken to begin encryption, Concentra's efforts were incomplete and inconsistent over time, leaving patient PHI vulnerable throughout the organization. OCR's investigation further found Concentra had insufficient security management processes in place to safeguard patient information.

In addition to the payment, Concentra has agreed to adopt a corrective action plan, which includes:

- completing a risk analysis of all systems that contain ePHI; and
- developing a risk management plan that reduces risks and vulnerabilities identified in the risk analysis.

Resolution Agreements with New York and Presbyterian Hospital and Columbia University

OCR entered into settlement agreements with New York and Presbyterian Hospital (NYP) and Columbia University (CU), which included resolution amounts totaling $4.8 million. OCR initiated an investigation of NYP and CU following their submission of a joint breach report regarding the disclosure of the ePHI of 6,800 individuals, including patient status, vital signs, medications, and laboratory results.

NYP and CU are separate covered entities that participate in a joint arrangement in which CU faculty members serve as attending physicians at NYP. The entities generally refer to their affiliation as "New York Presbyterian Hospital/Columbia University Medical Center." NYP and CU operate a shared data network and a shared network firewall that is administered by employees of both entities. The shared network links to NYP patient information systems containing ePHI.

The investigation revealed that the breach was caused when a physician employed by CU who developed applications for both NYP and CU attempted to deactivate a personally-owned computer server on the network containing NYP patient ePHI. Because of a lack of technical safeguards, deactivation of the server resulted in ePHI being accessible on Internet search engines. The entities learned of the breach after receiving a complaint by an individual who found the ePHI of the individual's deceased partner, a former patient of NYP, on the Internet.

In addition to the impermissible disclosure of ePHI on the Internet, OCR's investigation found that neither NYP nor CU made efforts prior to the breach to assure that the server was secure and that it contained appropriate software protections. Moreover, OCR determined that neither entity had conducted an accurate and thorough risk analysis that identified all systems that access NYP ePHI. As a result, neither entity had developed an adequate risk management plan that addressed the potential threats and hazards to the security of ePHI. Lastly, NYP failed to implement appropriate policies and procedures for authorizing access to its databases and failed to comply with its own policies on information access management.

NYP has paid OCR a monetary settlement of $3,300,000 and CU $1,500,000, with both entities agreeing to a substantive corrective action plan, which included:

- undertaking a risk analysis;
- developing a risk management plan;
- revising policies and procedures;
- training staff; and
- providing progress reports to OCR.

Resolution Agreement with Anchorage Community Mental Health Services

Anchorage Community Mental Health Services (ACMHS) agreed to settle potential violations of the HIPAA Security Rule with OCR. ACMHS paid $150,000 and adopted a corrective action plan to correct deficiencies in its HIPAA compliance program. ACMHS is a five-facility,

nonprofit organization providing behavioral health care services to children, adults, and families in Anchorage, Alaska.

OCR opened an investigation after receiving notification from ACMHS regarding a breach of unsecured electronic protected health information (ePHI) affecting 2,743 individuals due to malware compromising the security of its information technology resources. OCR's investigation revealed that ACMHS had adopted sample Security Rule policies and procedures in 2005, but these were not followed. Moreover, the security incident was the direct result of ACMHS failing to identify and address basic risks, such as not regularly updating their IT resources with available patches and running outdated, unsupported software.

ACMHS cooperated with OCR throughout its investigation and has been responsive to technical assistance provided to date. In addition to the settlement amount, the agreement includes a corrective action plan that requires ACMHS to:

- revise and distribute policies and procedures to all workforce members;
- train all workforce members; and
- conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI within its possession.

OCR Audits of the Privacy, Security and Breach Notification Rules

The American Recovery and Reinvestment Act of 2009 (ARRA), in Section 13411 of the Health Information Technology for Economic and Clinical Health Act (HITECH Act), requires HHS to perform periodic audits of covered entity and business associate compliance with the 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. The objectives of the audits are to: 1) assess entity compliance efforts with regard to the provisions of the Rules, 2) ensure covered entities and business associates are adequately safeguarding PHI, and 3) ensure individuals are provided the rights afforded to them by the Rules. The mechanisms by which we plan to achieve these objectives are to analyze an entity's key policies, procedures, and related processes and controls relative to requirements specified in the audit protocol.

The audit program is an important component of OCR's overall health information privacy and security compliance program. OCR uses the audit program to assess HIPAA compliance efforts across a broad range of covered entities and business associates. Audits present an 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.

Through the use of funds available under HITECH, OCR engaged the services of a professional public accounting firm to conduct the pilot audit program in 2011-2012. As part of this pilot,

OCR established a comprehensive audit protocol containing the HIPAA regulatory requirements to be assessed in the audits.

Throughout 2013, OCR analyzed the findings of the pilot audits to uncover trends, potential best practices, and vulnerabilities. In addition, OCR engaged Price Waterhouse Cooper (PWC) to conduct an evaluation of the pilot audit program. The evaluation included surveys of audited entities, review of the protocols, and examination of the audit program structure and documentation. OCR received the final report from PWC in November 2013.

In 2014, OCR engaged in preparations for the second phase of the audit program. For example, OCR revised its screening questionnaire intended to gather data about the size, complexity, and operations of potential auditees; this data will help OCR make audit subject selections in a way that is objective and, to the extent possible, representative of a broad cross section of entities covered by HIPAA. OCR also began updating the audit protocol to reflect the new regulatory requirements implemented through the January 25, 2013, Omnibus final rule and to assure that phase 2 of the program could include audits of both covered entities and business associates. Other activities in 2014 included development of additional guidance responsive to issues found through the pilot audits.

OCR launched phase 2 of the audit program in 2016; further details of those audits will be included in subsequent reports.

Lessons Learned

Much can be learned from the breach reports in terms of areas of vulnerability with respect to 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. A thorough and enterprise-wide risk analysis is the cornerstone of any HIPAA compliance program. Covered entities and business associates must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all electronic protected health information (ePHI) created, maintained, received or transmitted by their organizations. Covered entities and business associates frequently underestimate the proliferation of ePHI within their environments. When identifying ePHI, covered entities and business associate should consider:
    - Applications (EHR, PM, billing systems; documents and spreadsheets; database systems and web servers; fax servers, backup servers; etc.);
    - Computers (servers, workstations, laptops, virtual and cloud based systems, etc.);
    - Medical Devices (tomography, radiology, DXA, EKG, ultrasounds, spirometry, etc.);
    - Messaging Applications (email, texting, ftp, etc.)
    - Mobile and Other Devices (tablets, smartphones, copiers, digital cameras, etc.);
    - Media (tapes, CDs/DVDs, USB drives, memory cards, etc.).

- Risk Management. The Risk Management Standard requires the implementation of security measures sufficient to reduce risks and vulnerabilities that are identified (or should have been identified) in the risk analysis to a reasonable and appropriate level to comply with the Security Rule. Investigations conducted by OCR after several breaches uncovered that entities had failed to implement appropriate security measures to address risks that had been identified in their risk analyses, and that failure contributed to the breach. Covered entities and business associates should ensure that their risk management plans are thorough, and have addressed the potential risks and vulnerabilities to all ePHI in the environment, regardless of location or media (as described above).

- Encryption. The HIPAA Security Rule requires that covered entities and business associates encrypt their ePHI or implement reasonable compensating controls if encryption is determined infeasible for their enterprises. Further, the HIPAA Breach Notification Rule provides a safe harbor from breach notification if ePHI in a breach is encrypted. Nevertheless, based on breach reports and OCR's investigations, many covered entities and business associates are not encrypting their ePHI. In some cases, encryption was included as part of a remediation plan; however, activities to implement encryption were not carried out or were not implemented within a reasonable timeframe as established in the plan.

- Transmission Security. When electronically transmitting ePHI, covered entities and business associates must implement technical security measures or mechanisms to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network. This may require covered entities and business associates to encrypt the ePHI. Applications for which transmission security should be considered include: email; texting; application sessions; file transmissions (e.g., ftp); and remote access and support sessions (e.g., VPN).

- Security Evaluation. Covered entities and business associates must 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 administrative, 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. Similarly, covered entities and business associates must conduct appropriate technical evaluations, including testing, where there are technical upgrades for software, hardware, and websites or other changes to information systems or implementation of new technologies to ensure ePHI will not be at risk when the changes are implemented.

- Security and Control of Portable Electronic Devices. Covered entities and business associates must ensure that PHI that is stored and transported on portable electronic devices is properly safeguarded, including through encryption where appropriate. Such entities also must 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. Covered entities and business associates must implement clear policies and procedures for the proper disposal of PHI in all forms. Many breaches occur when entities improperly dispose of paper PHI. For electronic devices and equipment that store ePHI, covered entities and business associates must 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.

- Training. Covered entities and business associates must ensure employees are trained on their privacy and security policies and procedures, including the appropriate uses and disclosures of PHI; emerging threats to ePHI, such as malware and ransomware; and the safeguards that should be implemented to protect the information from improper uses and disclosures. Covered entities and business associates must also implement their sanctions policies so that employees are aware of the consequences for failure to follow the organization's policies and procedures.

Summary and Conclusion

For breaches occurring in 2013 and 2014, breaches involving 500 or more individuals made up 0.65 percent of reports (571 reports affecting 500 or more individuals out of 87,278 total reports), yet accounted for 98.44 percent of the individuals who were affected by a breach of their PHI (29,515,862 individuals out of a total of 29,982,339 individuals). In 2011 and 2012, breaches affecting 500 or more individuals made up less than one percent of reports, but accounted for more than 97 percent of the individuals affected by a breach of their PHI. As such, less than one percent of breaches reported affect the vast majority of individuals affected by breaches. OCR invests the majority of its resources in investigation of the breaches affecting the greatest number of individuals. In 2013 and 2014, theft and loss of PHI 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 affect the greatest number of 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/hipaa/for-professionals/breach-notification/index.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 2014, OCR had opened investigations into over 1854 breaches, including the 571 breaches affecting 500 or more individuals that occurred in 2013 and 2014. 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 ten cases resulting from a breach report, the Department has entered into resolution agreements/corrective action plans totaling more than $10 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.