Report to Congress on
Breaches of Unsecured Protected Health Information

For Calendar Years 2015, 2016, and 2017

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 2015, 2016, and 2017.[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 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] This Report to Congress covers a 3-year period. Future reports will be issued yearly. 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 entity 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.[3] 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.

[3] The Breach Notification Rule requires business associates to report to the covered entity the breach of unsecured PHI within 60 days of discovery. Through the business associate agreement, the parties may add additional specificity regarding the breach notification obligations of the business associate, such as a stricter timeframe for the business associate to report a potential breach to the covered entity and/or whether the business associate will handle breach notifications to individuals, HHS, and potentially the media, on behalf of the covered entity.

- **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. It must 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. 45 CFR § 164.408(b). 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(c). Covered entities must notify the Secretary by filling out and electronically submitting a breach report form on the Department website 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, pursuant to agreement with its business associate(s), 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, 2015, and December 31, 2017 and describes actions that have been taken by covered entities and business associates in response to the reported breaches.

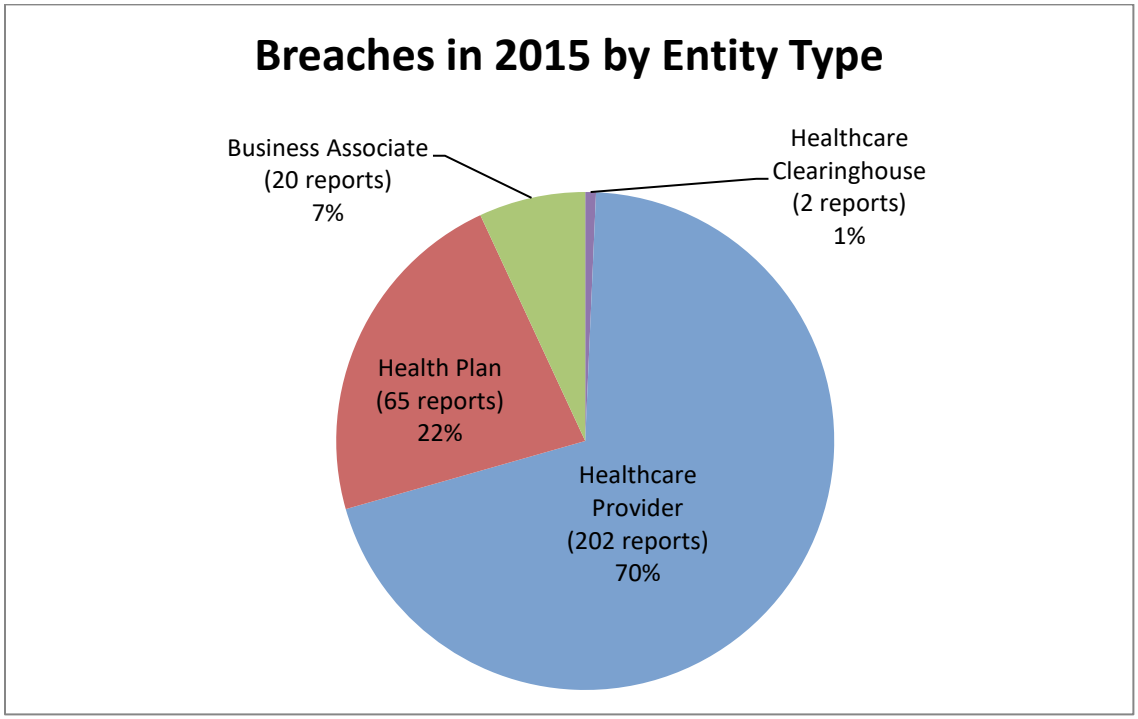
In addition, this report generally describes the OCR investigations and enforcement actions with respect to the reported breaches. Additional information on OCR's compliance and enforcement efforts in other areas may be found in OCR's Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance for Calendar Years 2015, 2016, and 2017. 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 2015, 2016 and 2017, the Department entered into twenty-one resolution agreements/corrective action plans or imposed civil money penalties totaling more than $42 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 289 reports of such breaches for calendar year 2015,[4] which affected a total of approximately 110,702,718 individuals.[5] For breaches occurring in calendar year 2016, OCR received 334 reports of such breaches, which affected a total of approximately 14,570,043 individuals. For breaches occurring in calendar year 2017, OCR received 385 reports of such breaches, which affected a total of approximately 5,747,019 individuals.

Breaches in 2015 Affecting 500 or More Individuals

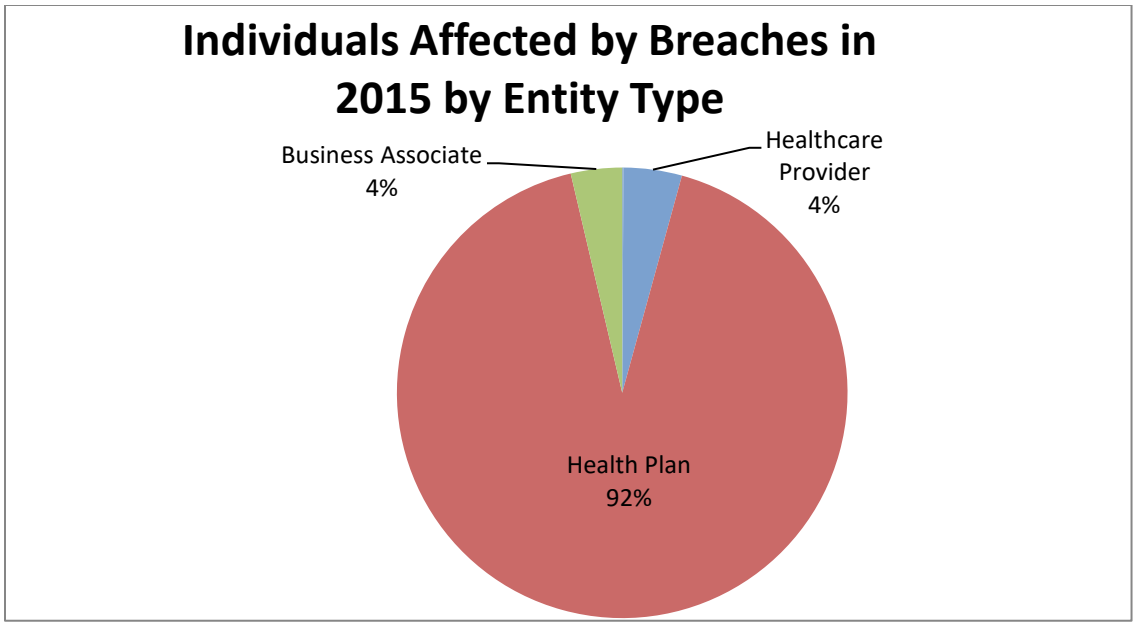
For the 289 breaches in 2015 affecting 500 or more individuals, OCR received 202 reports (70%) of breaches from healthcare providers (affecting a total of 4,630,245 individuals (4%)); 65 reports (22%) of breaches from health plans (affecting a total of 101,905,017 individuals (92%)); two reports (1%) of breaches from clearinghouses (affecting a total of 100,500[6] individuals); and 20 reports (7%) of breaches from business associates (affecting a total of 4,066,956 individuals (7%)).



[4] The Department receives some reports where the breach occurred over a 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 2015 into 2016 would be reported with the 2016 numbers.

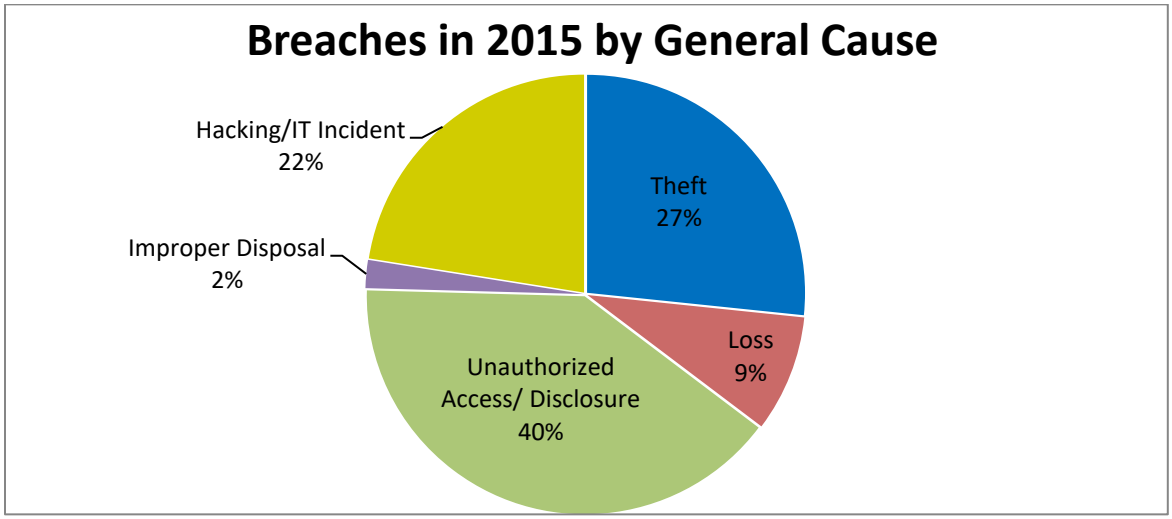
[5] The numbers of affected individuals provided throughout this report are approximate because some covered entities reported uncertainty about the number of records affected by a breach.

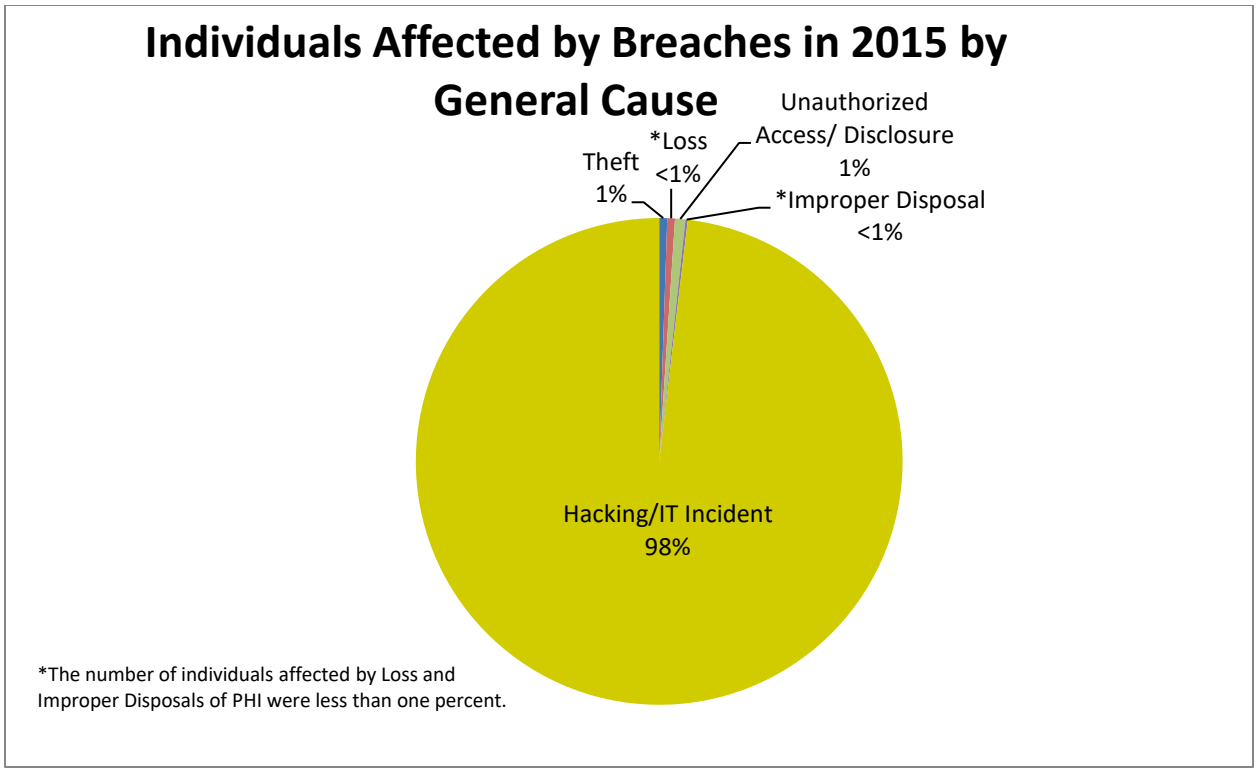
[6] Throughout this report, in instances in which the percentage is less than one, the percentage is not reported.



The 289 reports for breaches occurring in 2015 are categorized by five general causes as follows (in order of frequency):

(1) Unauthorized access or disclosure of records containing PHI (116 reports (40%) affecting 756,120 individuals (1%));
(2) Theft of electronic equipment/portable devices or paper containing PHI (77 reports (27%) affecting 583,761 individuals (1%));
(3) Hacking/IT incident of electronic equipment or a network server (65 reports (22%) affecting 108,623,928 individuals (98%));
(4) Loss of electronic media or paper records containing PHI (25 reports (9%) affecting 565,106 individuals (1%)); and
(5) Improper disposal of PHI (6 reports (2%) affecting 173,803 individuals).



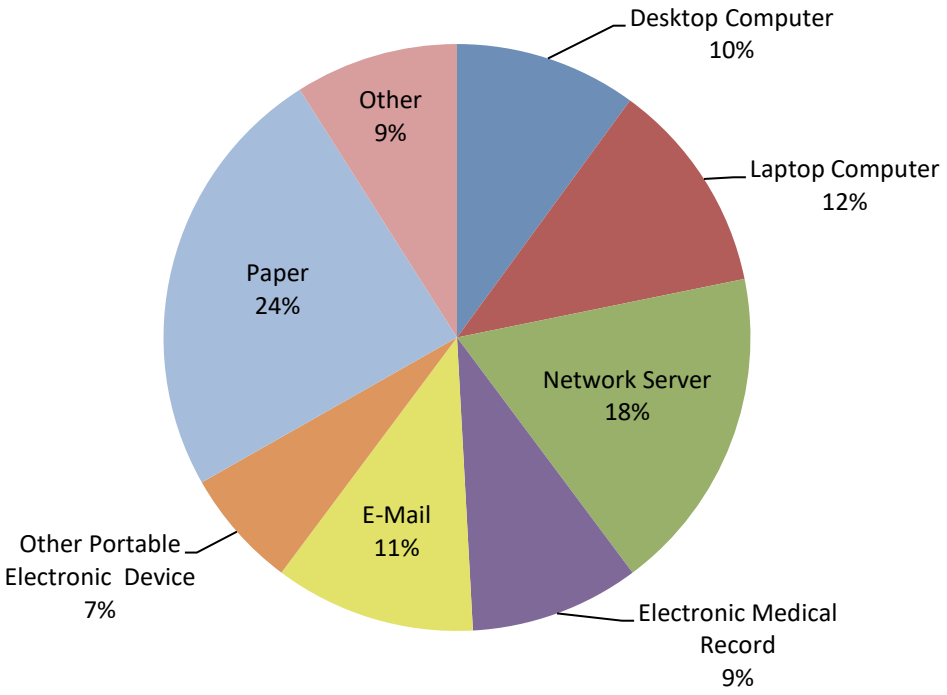


The 289 reports for breaches occurring in 2015 described the following locations of the PHI (in order of frequency):

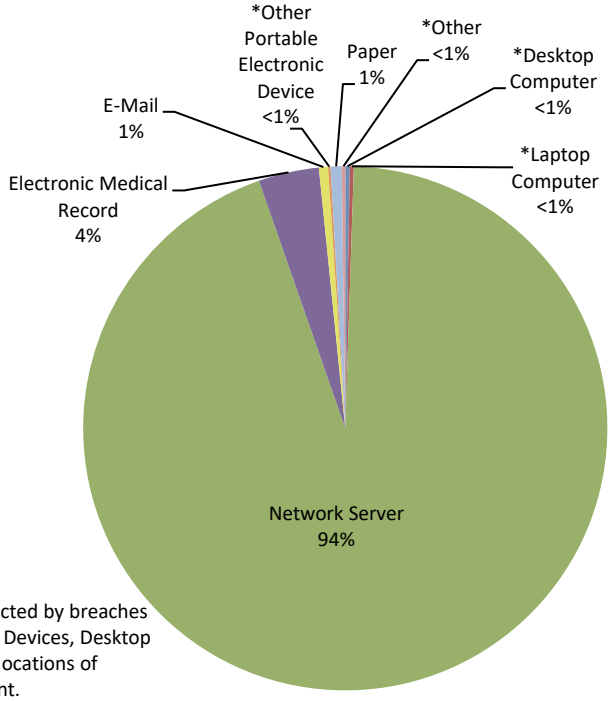
(1) Paper (70 reports (24%) affecting 754,262 individuals (1%);
(2) Network server (52 reports (18%) affecting 104,209,584 individuals (94%));
(3) Laptop (34 reports (12%) affecting 270,761 individuals);
(4) E-mail (32 reports (11%) affecting 623,281 individuals (1%));
(5) Desktop (29 reports (10%) affecting 307,143 individuals);
(6) Electronic medical record (27 reports (9%), affecting 4,131,700 individuals (4%));
(7) Other (26 reports (9%) affecting 235,834 individuals); [7] and
(8) Other portable electronic device (19 reports (7%) affecting 170,153 individuals).

[7] Other is used when a covered entity is unable to identify the specific location of the breach, such as when an impersonator accesses data or data is taken by and employee but the covered entity is not certain of the PHI's location when it was accessed.

Breaches in 2015 by Location of PHI



Individuals Affected by Breaches in 2015 by Location of PHI



*The percentage of individuals affected by breaches involving Other Portable Electronic Devices, Desktop and Laptop Computers, and Other locations of breaches were less than one percent.

Largest breaches in 2015 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.

Hacking/IT Incident of Electronic Equipment or Network Server: The largest breach in 2015 was the result of a hacking/IT incident involving a covered entity affecting over 78 million individuals. A cyber-attack disrupted its computer systems and servers. Other hacking/IT incidents involved the use of malware to gain access to computer systems, ransomware attacks, employees opening e-mail attachments that contain viruses, and the posting of PHI to public websites.

Theft: The largest theft in 2015, was the result of a burglary affecting 71,036 individuals. The covered entity discovered that an employee's vehicle was broken into and an unencrypted laptop was stolen. In most reported theft cases, laptops were stolen from vehicles; a vast majority of the laptops were compromised due to the lack of proper security measures.

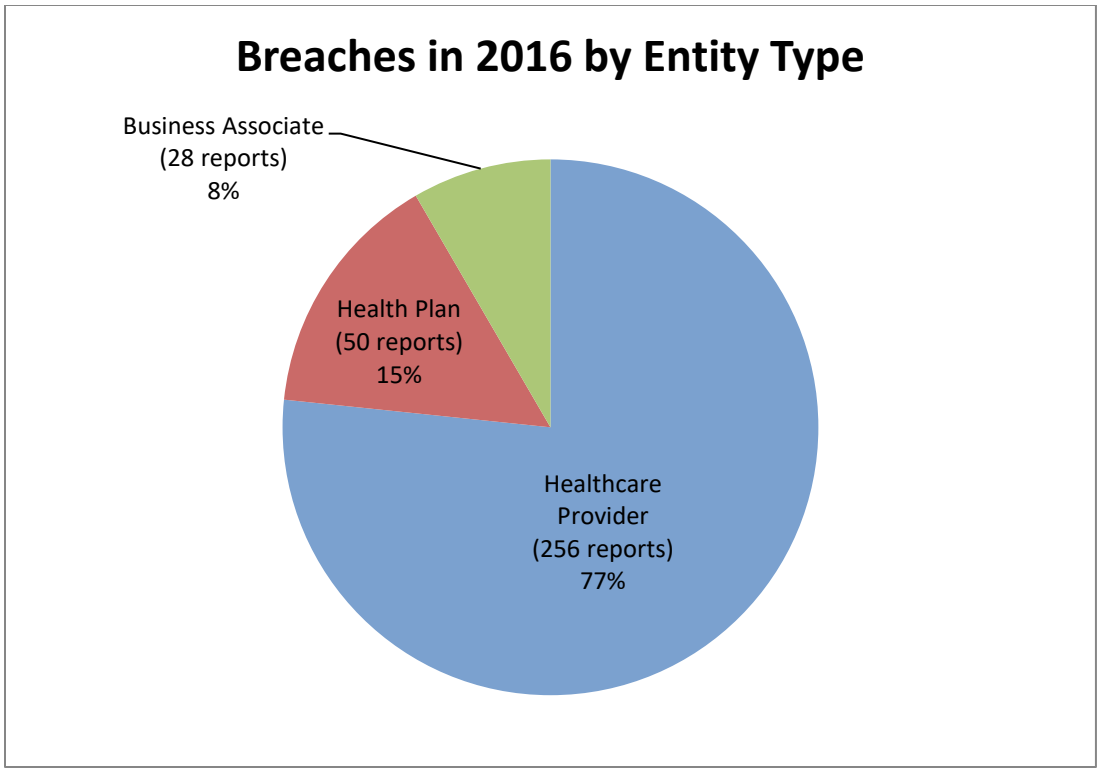
Improper Disposal: The largest improper disposal breach for 2015 involved the disposal of medical records affecting approximately 113,528 individuals. In this case, the covered entity did not properly dispose of medical records which contained PHI. Law enforcement contacted the covered entity and informed them that the medical records of numerous patients were found in a dumpster. Most of the improper disposal cases involving paper records were the result of employees improperly disposing of documents containing PHI in regular containers rather than authorized shredding containers.

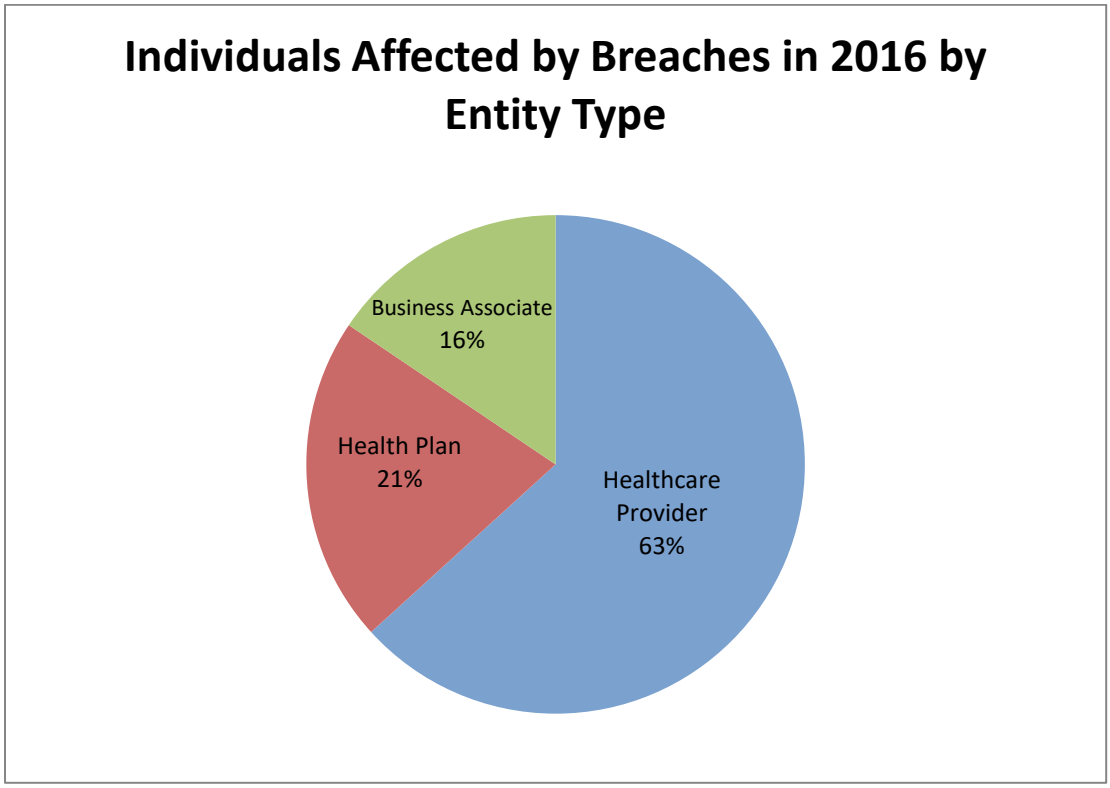
Unauthorized Access or Disclosure: The largest breach reported by an entity in 2015 involving the unauthorized access or disclosure of PHI occurred when a spreadsheet containing Medicaid information was impermissibly emailed to another employee affecting 141,288 individuals. Other reports of unauthorized access or disclosure of PHI involved mailing errors, as well as employees viewing or removing PHI for purposes beyond the scope of their duties.

Loss of PHI: The largest breach as a result of a loss for 2015 involved an unencrypted flash drive that the covered entity discovered was missing from its office, affecting approximately 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.

Breaches in 2016 Affecting 500 or More Individuals

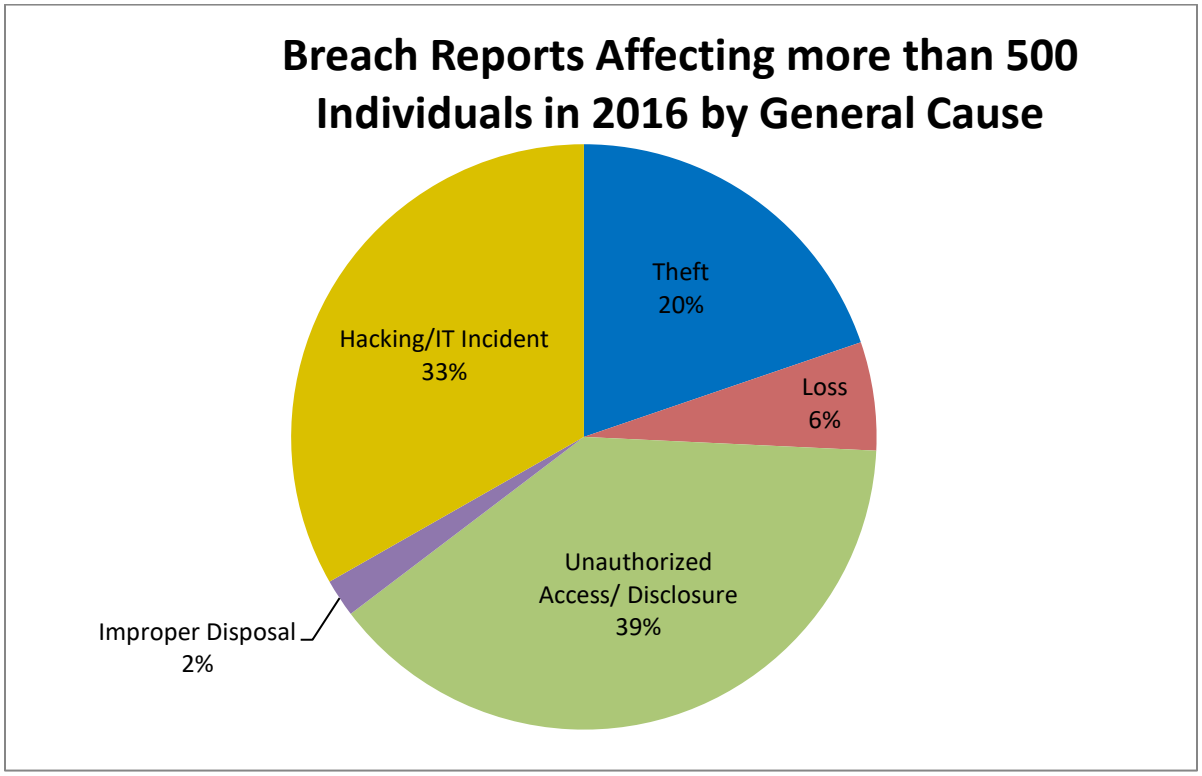
For the 334 breaches affecting 500 or more individuals in 2016, OCR received 256 reports (77%) of breaches from healthcare providers (affecting a total of 9,217,128 (63%) of individuals); 50 reports (15%) of breaches from health plans (affecting a total of 3,084,691 (21%) of individuals); and 28 reports (8%) of breaches from business associates (affecting a total of 2,268,224 (16%) of individuals.


Breaches in 2016 by Entity Type
Business Associate
(28 reports)
8%
Health Plan
(50 reports)
15%
Healthcare
Provider
(256 reports)
77%

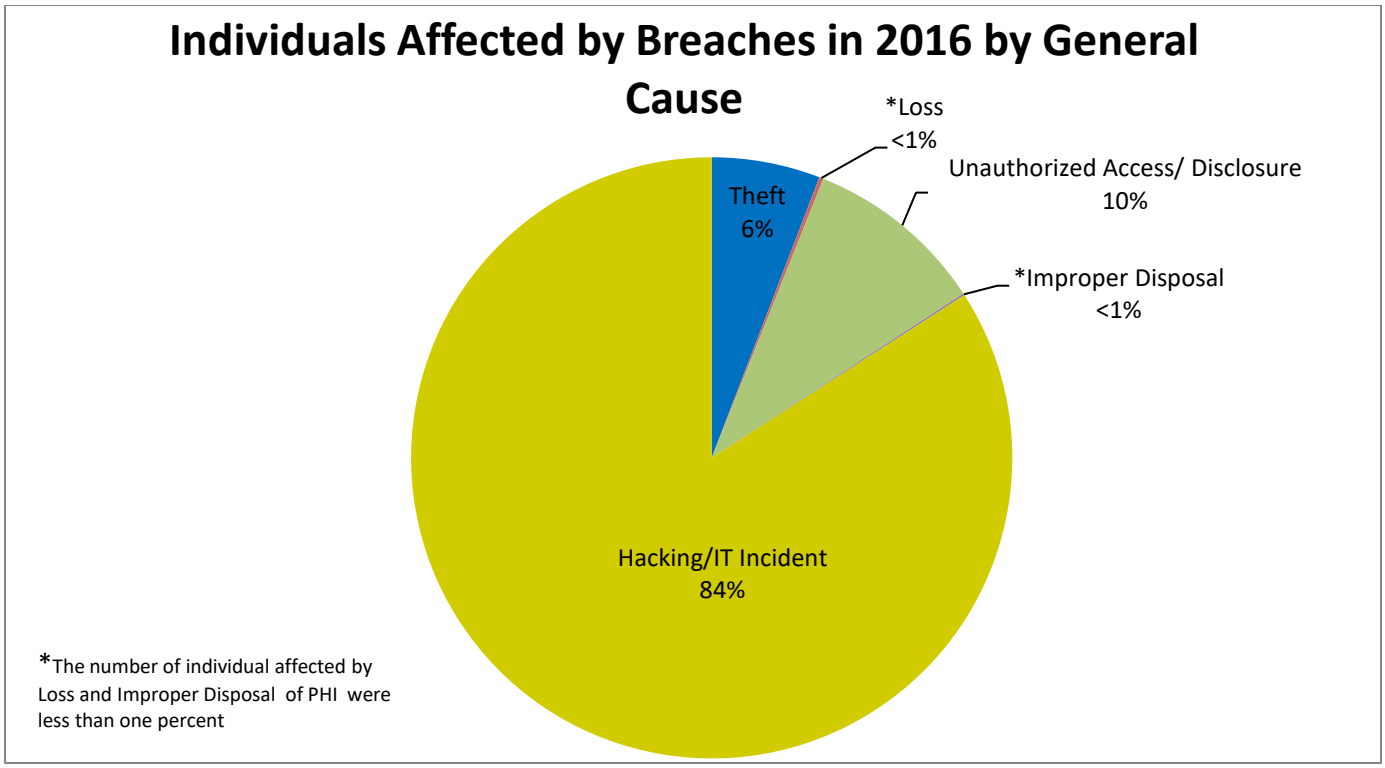

Individuals Affected by Breaches in 2016 by Entity Type
Business Associate
16%
Health Plan
21%
Healthcare
Provider
63%

The 334 reports submitted to OCR for breaches affecting 500 or more individuals occurring in 2016 can be categorized by five general causes of incidents as follows (in order of frequency):

(1) Unauthorized access or disclosure of records containing PHI (130 reports (39%) affecting 1,418,825 individuals (10%);
(2) Hacking/IT incident of electronic equipment or a network server (111 reports (33%) affecting 12,254,431 (84%) of individuals);
(3) Theft of electronic equipment/portable devices or paper containing PHI (66 reports (20%) affecting 850,092 individuals (6%));
(4) Loss of electronic media or paper records containing PHI (20 reports (6%) affecting 33,006 individuals[8]); and
(5) Improper disposal of PHI (seven reports (2%) affecting 13,689 individuals).

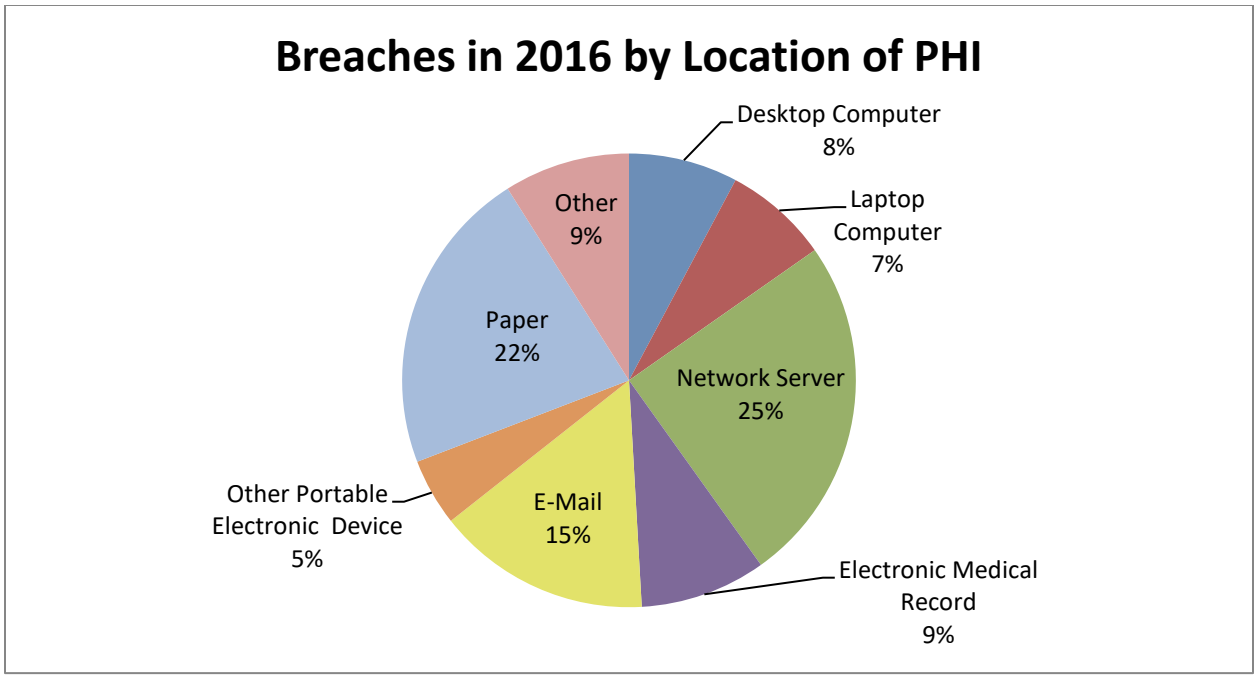


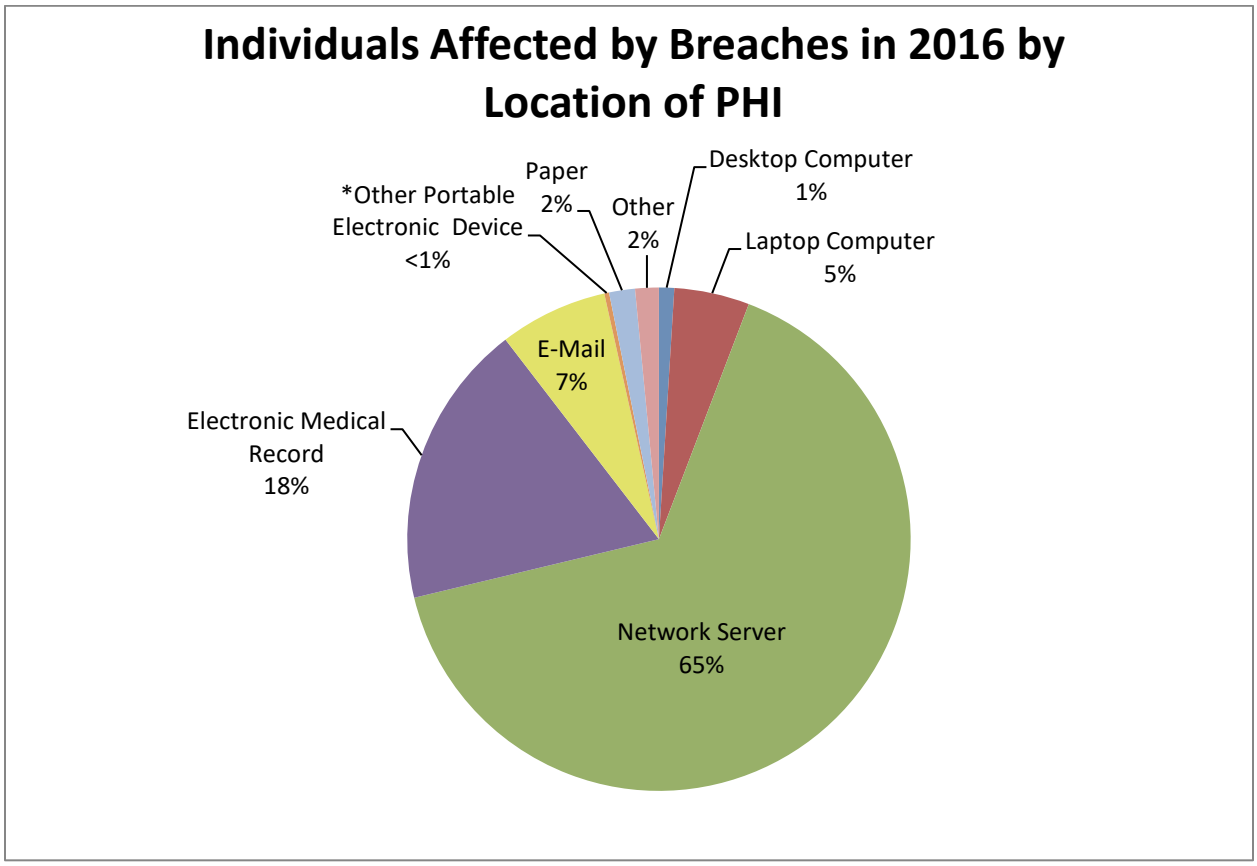
[8] In instances in which the percentage is less than one, the percentage is not reported.



The 334 reports submitted to OCR for breaches occurring in 2016 described the following locations of the PHI (in order of frequency):

(1) Network server (83 reports (25%) affecting 9,535,395 individuals (65%));
(2) Paper (73 reports (22%) affecting 242,106 individuals (2%));
(3) E-mail (51 reports (15%) affecting 1,012,575 individuals (7%));
(4) Electronic medical record (30 reports (9%) affecting 2,667,310 individuals (18%));
(5) Other (30 reports (9%) affecting 220,913 individuals (2%));
(6) Desktop computer (26 reports (8%) affecting 142,730 individuals (1%));
(7) Laptop computer (25 reports (7%) affecting 704,278 individuals (5%)); and
(8) Other portable electronic device (16 reports (5%) affecting 44,736 individuals).





*****The percentage of individuals affected by breaches involving Other Portable Electronic Devices were less than one percent.

Largest breaches in 2016 for each reported cause

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

Hacking/IT Incident of Electronic Equipment or Network Server: The largest breach in 2016 resulting from a hacking/IT incident involved a cyber-attack in which hackers penetrated multiple servers affecting approximately 3,620,000 individuals. Other hacking/IT incidents involved covered entities that discovered viruses or malware, ransomware attacks, or unidentified, unauthorized persons obtaining access to systems.

Theft: The largest breach in 2016 resulting from theft involved an unencrypted laptop that was stolen from an employee's vehicle affecting approximately 400,000 individuals.

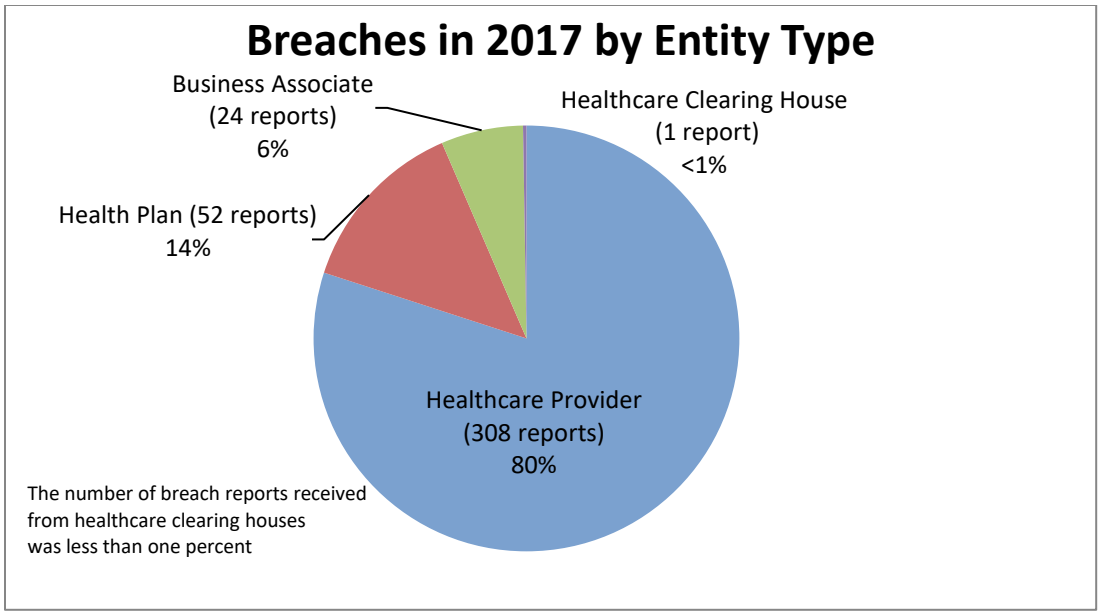
Improper Disposal: The largest reported incident in 2016 involving improper disposal resulted from the improper disposal of dental records affecting 5,600 individuals. An investigation by a covered entity revealed that several employees were responsible for dumping dental records in a dumpster as part of a clean-up effort. Other improper disposal breaches involved paper records containing PHI disposed of in recycling or trash bins rather than shred bins.

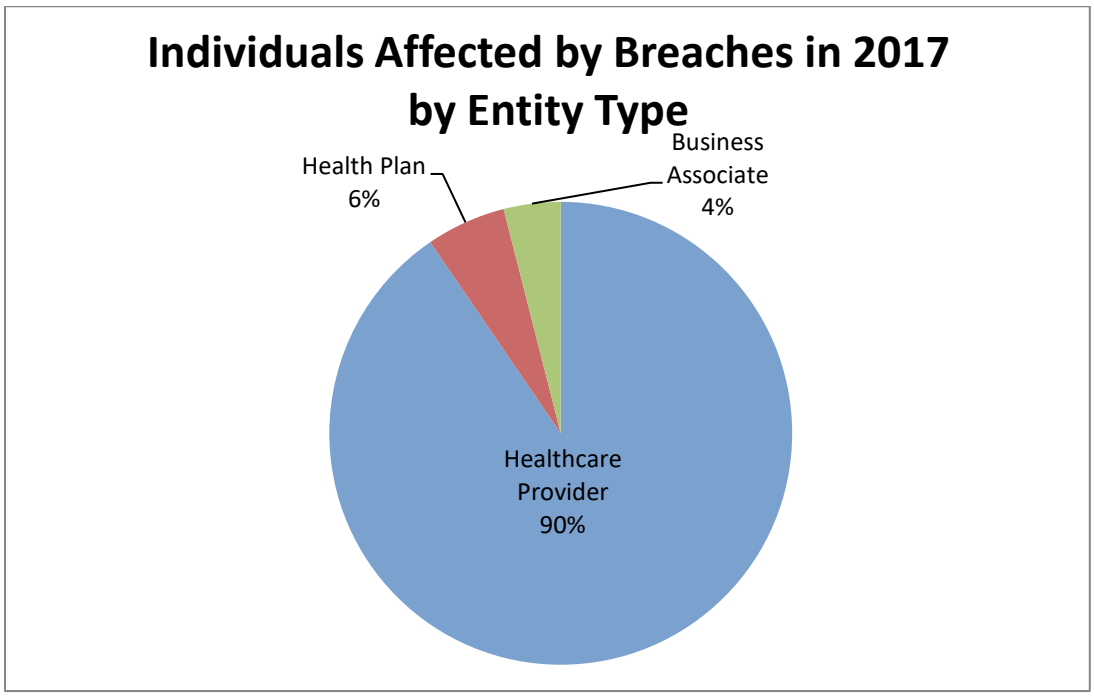
Unauthorized Access or Disclosure of PHI: The largest breach in 2016 involving the unauthorized access or disclosure of PHI affected approximately 655,000 individuals. In this case, a covered entity discovered that PHI of its patients was accessible via the Internet. Other incidents of unauthorized access or disclosure involved employees impermissibly accessing records outside the scope of their job responsibilities, emailing PHI without encryption, and misdirected communications.

Loss of PHI: The largest breach reported as a loss in 2016 resulted from the loss of 139 boxes of medical records during transport from one storage facility to another affecting approximately 6,786 individuals.

Breaches in 2017 Affecting 500 or More Individuals

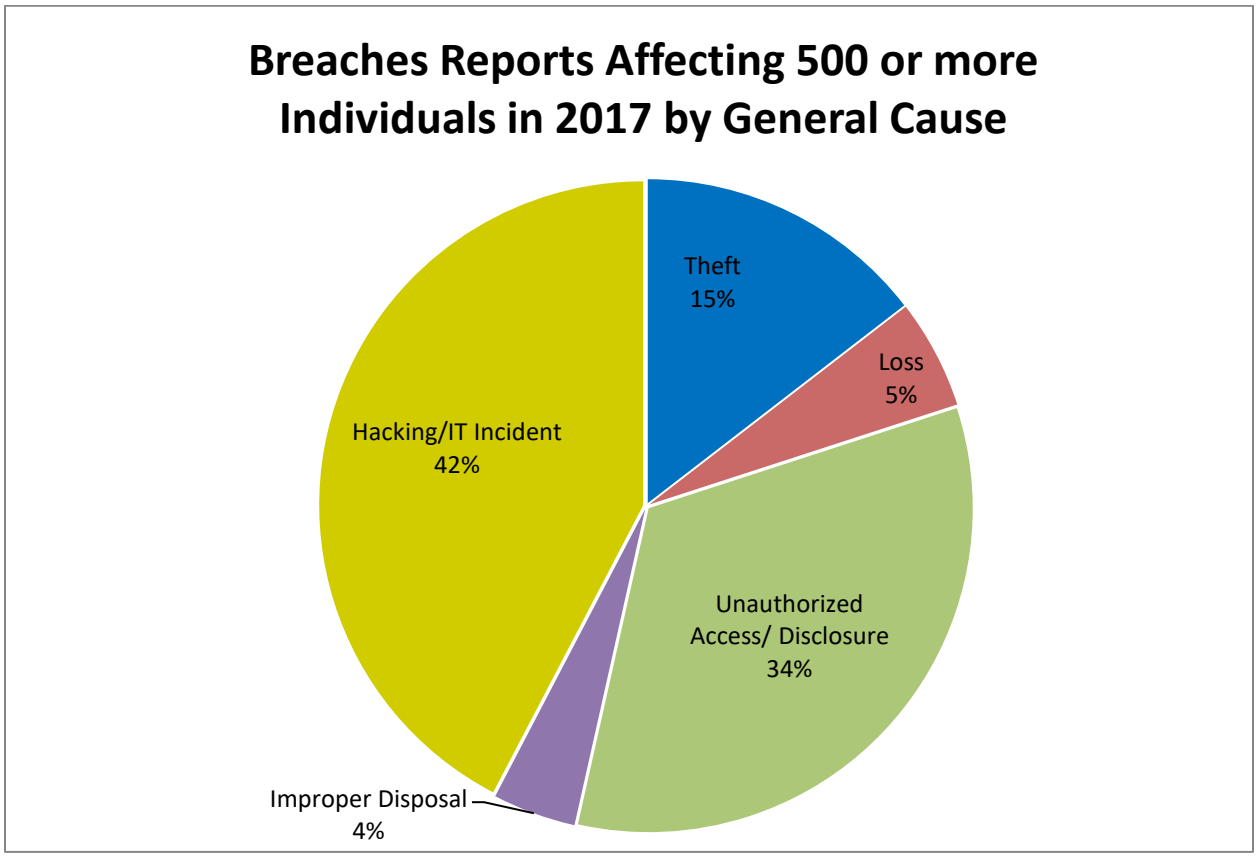
For the 385 breaches affecting 500 or more individuals in 2017, OCR received 308 reports (80%) of breaches from health care providers (affecting 5,198,029 individuals (90%)); 52 reports (14%) of breaches from health plans (affecting 319,684 individuals (6%)); and 24 reports (6%) of breaches from business associates (affecting 228,174 individuals (4%)), and one report from a health care clearing house (affecting 1,132 individuals).

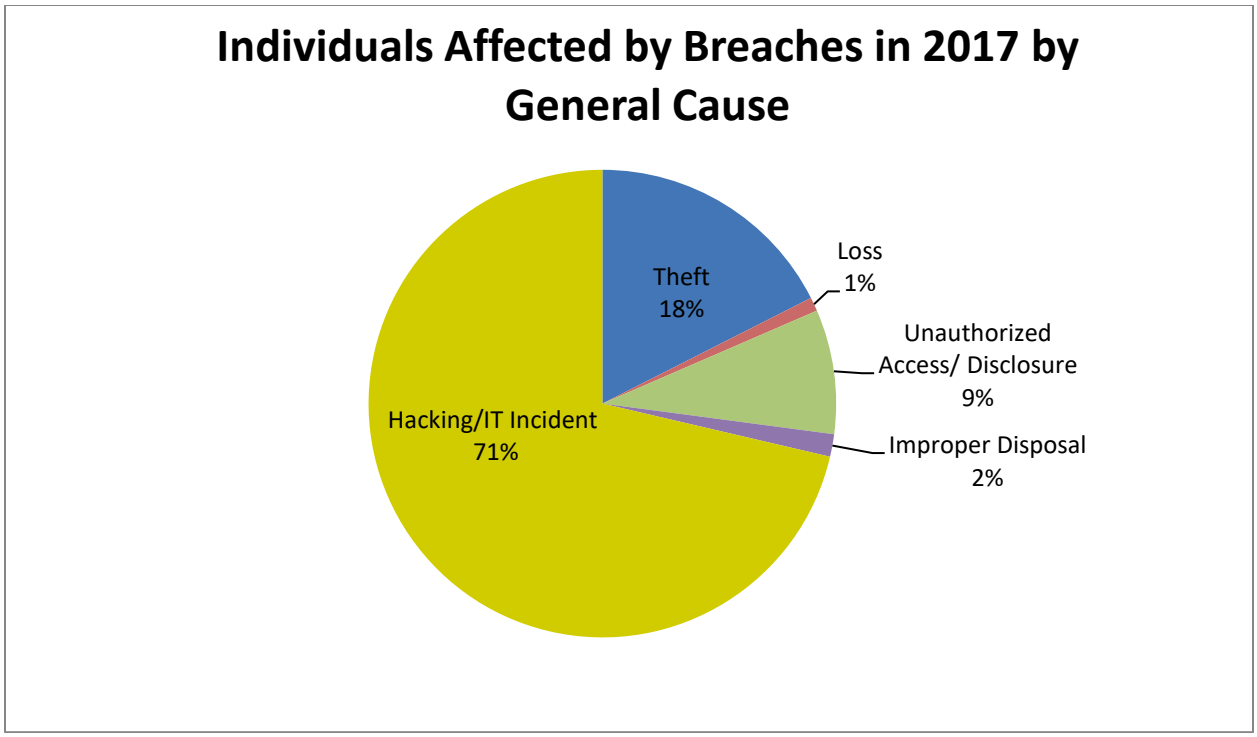




The 385 reports submitted to OCR for breaches affecting 500 or more individuals occurring in 2017 can be categorized by five general causes as follows (in order of frequency):

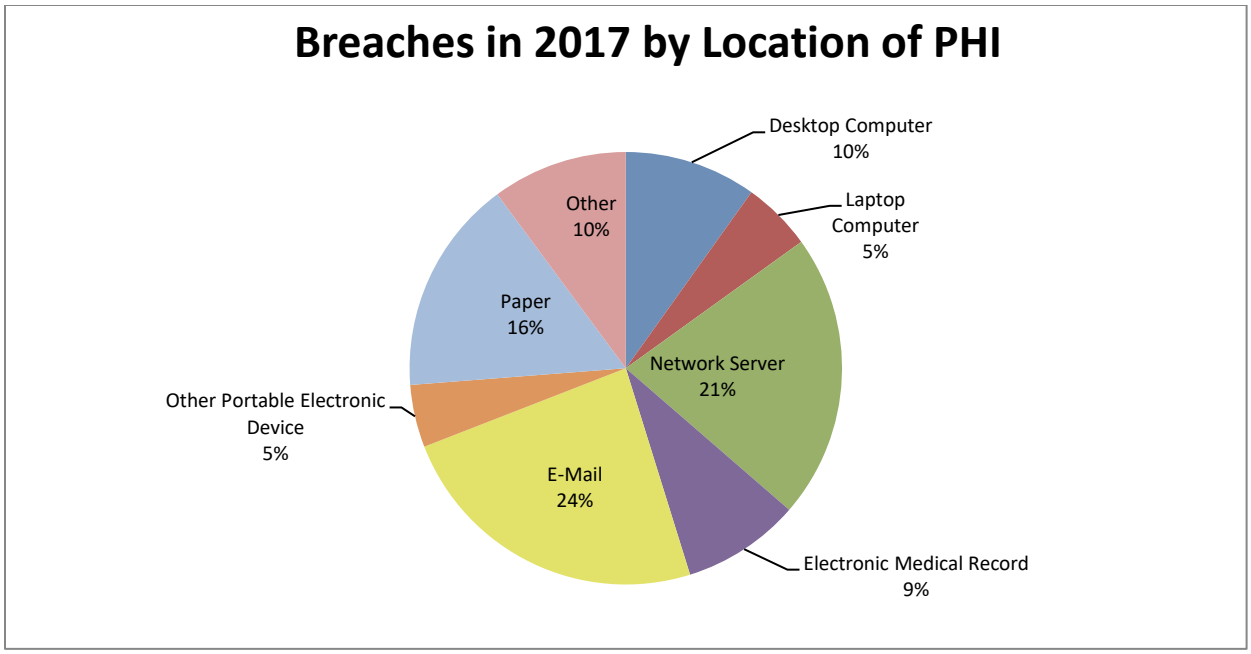
(1) Hacking/IT incident of electronic equipment or a network server (163 reports (42%) affecting 4,100,455 individuals (71%));
(2) Unauthorized access or disclosure of records containing PHI (129 reports (34%) affecting 494,479 individuals (9%));
(3) Theft of electronic equipment/portable devices or paper containing PHI (56 reports (15%), affecting 1,007,894 individuals (18%));
(4) Loss of electronic media or paper records containing PHI (21 reports (5%) affecting 54,859 individuals (1%)); and
(5) Improper disposal of PHI (16 reports (4%) affecting 89,332 individuals (2%)).

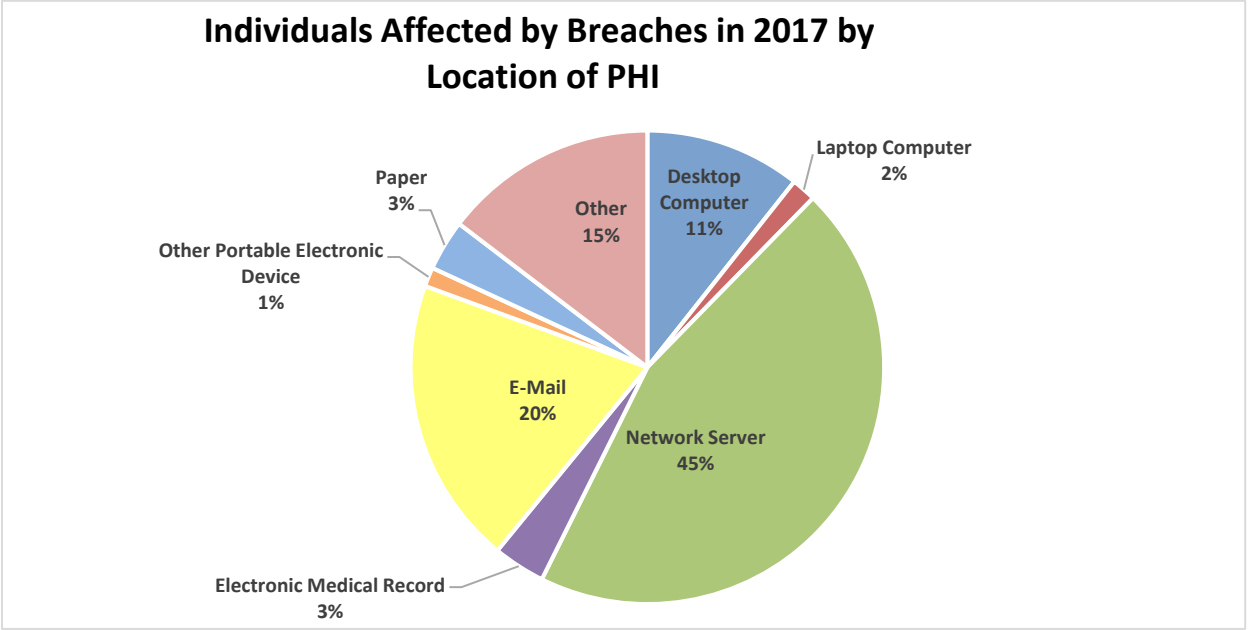




The 385 reports submitted to OCR for breaches occurring in 2017 described the following locations of the PHI (in order of frequency):

(1) E-mail (92 reports (24%) affecting 1,130,028 individuals (20%));
(2) Network server (82 reports (21%), affecting 2,587,241 individuals (45%));
(3) Paper (62 reports (16%) affecting 199,738 individuals (3%));
(4) Other (39 reports (10%) affecting 840,929 individuals (15%));
(5) Desktop computer (38 reports (10%) affecting 612,305 individuals (11%));
(6) Electronic medical record (34 reports (9%), affecting 204,954 individuals (4%));
(7) Laptop computer (20 reports (5%), affecting 96,496 individuals (2%)); and
(8) Other portable electronic device (18 reports (5%), affecting 75,328 individuals (1%)).





Largest breaches in 2017 for each reported cause

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

Hacking/IT Incident of Electronic Equipment or Network Server: The largest breach in 2017 resulting from a hacking/IT incident involved a ransomware cyber-attack in which a foreign criminal organization of hackers penetrated the server of a health care provider affecting approximately 500,000 individuals. Other hacking/IT incidents involved covered entities that

discovered viruses or malware, or were perpetrated by unidentified, unauthorized persons obtaining access to systems.

Theft: The largest breach in 2017 resulting from theft involved a thumb drive that was stolen from a health care organization affecting approximately 697,800 individuals.

Improper Disposal: The largest reported incident in 2017 involving improper disposal resulted from the improper disposal of medical records affecting 2,837 individuals. An investigation by a covered entity revealed that someone was responsible for dumping medical records along a highway that were subsequently discovered by a mail carrier. Other improper disposal breaches involved paper records containing PHI disposed of in recycling or trash bins rather than shred bins.

Unauthorized Access or Disclosure of PHI: The largest breach in 2017 involving the unauthorized access or disclosure of PHI affected approximately 56,075 individuals. In this case, a covered entity discovered that PHI of its patients was accessible via the Internet. Other incidents of unauthorized access or disclosure involved employees impermissibly accessing records outside the scope of their job responsibilities, emailing PHI without encryption, and misdirected communications.

Loss of PHI: The largest breach reported as a loss in 2017 resulted from the loss of medical records that were located in a storage facility affecting approximately 22,000 individuals.

Remedial Action Reported

For breaches affecting 500 or more individuals that occurred in 2015, 2016 and 2017, 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

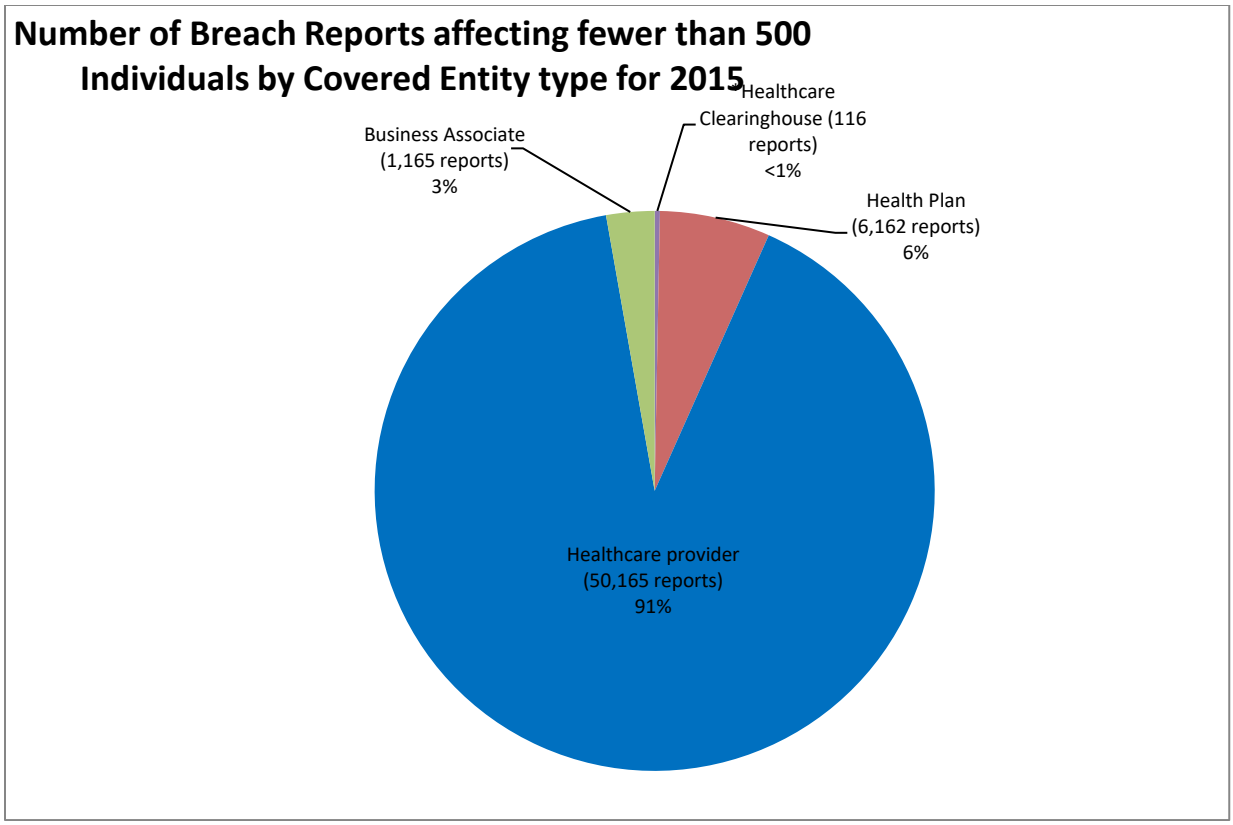
- Revising business associate contracts to include more detailed provisions for the protection of health information.

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 2015, notification to OCR was required no later than March 1, 2016. For breaches discovered during 2016, notification to OCR was required no later than March 1, 2017. For breaches discovered during 2017, notification to OCR was required no later than March 1, 2018.

Breaches involving fewer than 500 individuals for 2015

OCR received approximately 57,608 reports of smaller breaches that occurred between January 1, 2015, and December 31, 2015. These smaller breaches affected approximately 623,597 individuals. Of these reports of smaller breaches, 6,162 (11%) were reported by health plans (affecting 39,799 individuals (6%)); 50,165 (87%) were reported by healthcare providers (affecting 564,564 individuals (91%)); 116 reports were reported by healthcare clearinghouses (affecting 1873 individuals); and 1,165 reports (2%) were reported by business associates (affecting 17,361 (3%)).



*The percentage of individuals affected by breaches involving Healthcare Clearinghouses were less than one percent.

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

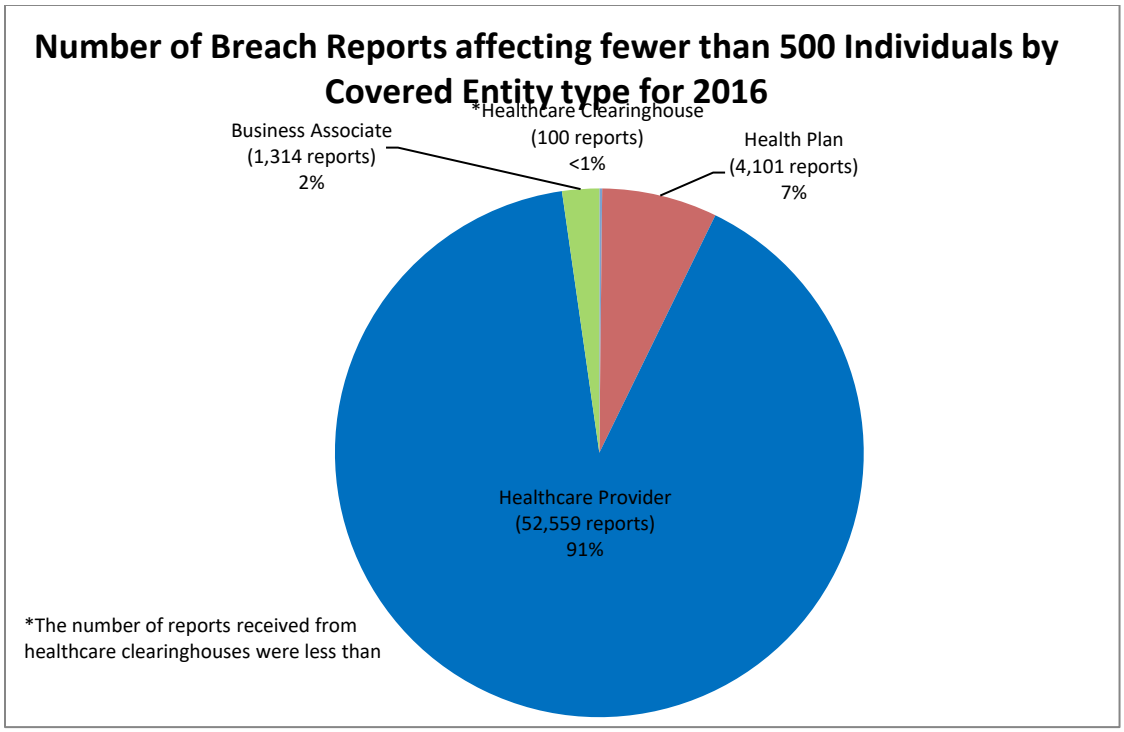
(1) Unauthorized access or disclosure (52,468 reports (91%) affecting 423,106 individuals (67%));
(2) Theft (2,313 reports (4%) affecting 11,091 individuals (2%));
(3) Loss (2,280 reports (4%) affecting 180,093 individuals (29%));
(4) Improper disposal (322 reports (1%) affecting 10,785 individuals (2%)); and
(5) Hacking/IT incident (225 reports affecting 6,681 individuals (1%)).

Of these reports, 38,078 reports (66%) involved paper records (affecting 138,156 individuals (22%)); 5,402 reports (9%) involved an electronic medical record (affecting 193,089 individuals (31%)); 2,250 reports (4%) involved e-mail (affecting 29,371 individuals (5%)); 790 reports (1%) involved a desktop computer (affecting 12,211 individuals (2%)); 690 reports (1%), involved portable electronic devices (affecting 12,672 individuals (2%)); 338 reports (1%) involved laptops (affecting 24,783 individuals (4%)); 333 reports (1%) involved network servers (affecting 14,253 individuals (2%)); and 9,727 reports (17%) (affecting 199,062 individuals (32%)) did not identify the location of the data that was breached.

Breaches involving fewer than 500 individuals for 2016

OCR received approximately 58,074 reports of smaller breaches that occurred between January 1, 2016, and December 31, 2016. These smaller breaches affected approximately 272,736 individuals. Of these reports of smaller breaches, 4,101 (7%) were reported by health plans

(affecting 35,957 individuals (13%)); 52,559 (91%) were reported by health care providers (affecting 216,300 individuals (79%)); 100 were reported by health care clearinghouses (affecting 862 individuals); and 1,314 (2%) were reported by business associates (affecting 19,617 individuals (7%)).



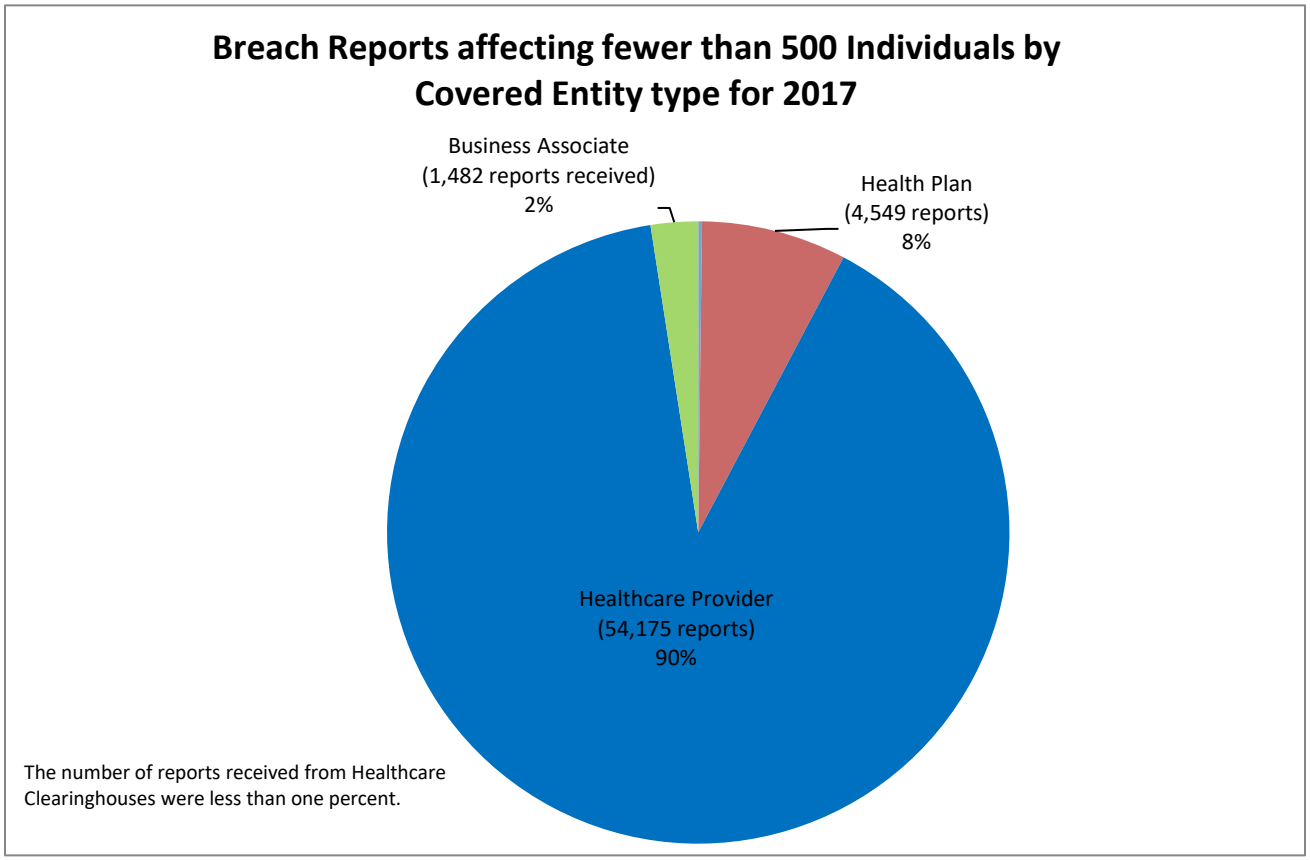
The most common causes of breach incidents (in order of frequency) for breaches affecting fewer than 500 individuals were:

(1) Unauthorized access or disclosure (54,253 reports (93%) affecting 246,104 individuals (90%));
(2) Loss (1,981 reports (3%) affecting 11,585 individuals (4%));
(3) Theft (1,295 reports (2%) affecting 3,638 individuals (1%));
(4) Improper disposal (275 reports affecting 2,206 individuals (1%)); and
(5) Hacking/IT incident (270 reports affecting 9,203 individuals (3%)).

Of these reports, 40,267 reports (69%) involved paper records (affecting 132,611 individuals (49%)); 5,576 reports (10%) involved an electronic medical record (affecting 22,958 individuals (8%)); 1,854 reports (3%) involved e-mail (affecting 30,509 individuals (11%)); 813 reports (1%)involved desktop computers (affecting 14,535 individuals (5%)); 790 reports (1%) involved portable electronic devices (affecting 11,710 individuals (4%)); 274 reports involved network servers (affecting 14,041 individuals (5%)); 268 reports involved laptops (affecting 15,108 individuals (6%)); and 8,232 reports (14%) did not identify the location of the data that was breached (affecting 31,264 individuals (11%)).

Breaches involving fewer than 500 individuals for 2017

OCR received 60,322 reports of smaller breaches that occurred between January 1, 2017, and December 31, 2017. These smaller breaches affected 270,329 individuals. Of these reports of smaller breaches, 54,175 (90%) were reported by health care providers (affecting 222,275 individuals (82%)); 4,549 (8%) were reported by health plans (affecting 31,711 individuals (12%)); 1,482 (2%) were reported by business associates (affecting 14,936 individuals (6%)) and 116 were reported by health care clearinghouses (affecting 1,407 individuals (1%)).



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

(1) Unauthorized access or disclosure (55,995 reports (93%) affecting 173,891 individuals (64%));
(2) Loss (2,386 reports (4%) affecting 23,823 individuals (9%));
(3) Theft (1,137 reports (2%) affecting 39,478 individuals (15%));
(4) Hacking/IT incident (454 reports (1%) affecting 22,262 individuals (8%)); and
(5) Improper disposal (350 reports (1%) affecting 10,875 individuals (4%)).

Of these reports, 40,623 reports (67%) involved paper records (affecting 122,617 individuals (45%)); 8,307 reports (14%) did not identify the location of the data that was breached (affecting 38,472 individuals (14%)); 6,964 reports (12%) involved an electronic medical record (affecting 26,925 individuals (10%)); 2,246 reports (4%) involved e-mail (affecting 40,669 individuals (15%)); 925 reports (2%) involved desktop computers (affecting 11,668 individuals (4%)); 760

reports (1%) involved portable electronic devices (affecting 7,306 individuals (3%)); 265 reports involved network servers (affecting 6,556 individuals (2%)); and 232 reports involved laptops (affecting 16,116 individuals (6%)).

Details on Breaches involving fewer than 500 individuals for 2015, 2016, and 2017

Incidents reported for 2015, 2016, and 2017 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. OCR completed 14 breach investigations involving fewer than 500 individuals in 2015, 17 in 2016, and 25 in 2017.

Cases Investigated and Action Taken

To fulfill its statutory obligation, OCR opened investigations into all of the 1008 breaches affecting 500 or more individuals that occurred in 2015, 2016, and 2017. OCR also opened 70 investigations into breaches affecting fewer than 500 individuals. OCR closed 882 investigations resulting from breach reports after achieving voluntary compliance, through corrective action and technical assistance, through resolution agreements, and because no violation had occurred. The specifics of the cases resulting in resolution agreements and civil money penalties can be found at the appendix at the end of this report. 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 2015, 2016, and 2017.

Lessons Learned

Breach reports offer insight into areas of vulnerability in protections for the privacy and security of individuals' health information. Covered entities and business associates should pay particular attention, in their compliance efforts, to the activities below to avoid some of the more common types of reported breaches.

- Protection from Malicious Software. Although many, if not most, covered entities and business associates employ some type of malicious software protection through anti-virus and anti-malware software, reliance on such solutions alone may not be enough. Hackers and malicious software increasingly target and exploit unpatched flaws and vulnerabilities in software (e.g., operating systems, applications, databases) and hardware (e.g., medical devices, storage appliances, network devices) to gain unauthorized access to systems and PHI. To protect against these attacks, entities must conduct a risk analysis to identify such threats and vulnerabilities within their environment, and implement

appropriate security measures (e.g., patching, applying stronger security configurations) through their risk management plans.

- Contingency Plan. Establishing contingency plans and implementing corresponding data backup, disaster recovery and emergency operations plans are all requirements of the HIPAA Security Rule. Natural disasters as well continuing cyberattacks such as ransomware highlight the criticality of robust contingency planning to ensure effective recovery in the healthcare sector following disasters.

- Access Control. Covered entities and business associates must implement technical access controls to ensure that access to PHI is restricted to only those persons and entities that are permitted to access PHI. It is important that entities consider not only whether access should be permitted, but also what type of access is reasonable and appropriate (e.g., read-only vs read-write). OCR's investigations uncover not only non-existent or inappropriate access controls, but also access controls that impede access for necessary and appropriate activities (e.g., gratuitous application of administrator or root privileges). Entities should have processes in place to periodically review access levels to ensure user access levels are appropriate and support core functions.

- Information System Activity Review. Recent breach reporting statistics show an increase of "Hacking/IT Incident" as the type of breach reported. If a malicious actor is able to defeat an organization's perimeter defenses and gain access to an organization's internal systems and networks, it is imperative that the organization have appropriate processes in place to review information system activity. Effective information system activity review processes can help identify malicious activity and alert the organization of an intruder. Once alerted, the organization can take appropriate actions to expel the intruder and remediate the vulnerabilities the intruder exploited to gain access. The HIPAA Security Rule requires covered entities and business associates to regularly review information system activity.

- Audit Controls. An effective information system activity review process requires effective audit controls. HIPAA requires the implementation of mechanisms to record and examine activity in information systems that contain or use ePHI. In addition to helping to identify malicious actors external to an organization, comprehensive audit logs that feed an effective review process can also identify the actions of malicious insiders (e.g., employees, contractors). The threat from malicious insiders is a prevalent and growing concern in the healthcare sector. Proper audit controls, along with an effective review process, can help identify and mitigate threats from malicious insiders.

- Security Incident Procedures. HIPAA requires covered entities and business associates to identify and respond to suspected or known security incidents. Non-existent or ineffective security incident procedures can prolong a breach and actions perpetrated by malicious actors. Robust and well-tested security incident procedures can prepare an organization to effectively respond to all manner of security incidents – be it a malicious insider, ransomware attack, or an Advanced Persistent Threat nation-state actor. Preparing for

how to respond to an incident after it happens can be just as important as how an entity prepares itself to prevent incidents.

Summary and Conclusion

For breaches occurring in 2015, 2016, and 2017, breaches involving 500 or more individuals made up 0.57 percent of reports (1008 reports affecting 500 or more individuals out of 177,012 reports), yet accounted for 99.12 percent of the individuals who were affected by a breach of their PHI (131,019,780 individuals out of a total of 132,186,442 individuals). As such, less than one percent of breaches reported affected the vast majority of individuals affected by breaches. OCR invests the majority of its resources in investigating the breaches affecting the greatest number of individuals. In 2015 and 2016, unauthorized access/disclosure and loss of PHI affected the largest numbers of individuals. In 2017, hacking/IT incidents and theft affected the largest numbers of individuals. Theft continues to be one of the top causes that affects 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 to 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 initiating 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 2017, OCR had opened investigations into over 4789 breaches, including the 1,008 breaches affecting 500 or more individuals that occurred in 2015, 2016, and 2017. OCR closed 726 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 mitigate any potential harm to affected individuals. During 2015, 2016 and 2017, in 21 cases resulting from breach reports, the Department entered into resolution agreements/corrective action plans or imposed civil money penalties totaling more than $42 million.

APPENDIX

Resolution Agreements and Civil Money Penalties in 2015, 2016, and 2017

Resolution Agreement with Cancer Care Group

Cancer Care Group (Cancer Care) agreed to settle potential violations of the HIPAA Privacy and Security Rules with OCR. Cancer Care paid $750,000 and agreed to adopt a robust corrective action plan to correct deficiencies in its HIPAA compliance program. Cancer Care Group is a radiation oncology private physician practice, with 13 radiation oncologists serving hospitals and clinics throughout Indiana.

On August 29, 2012, OCR received notification from Cancer Care regarding a breach of unsecured ePHI after a laptop bag was stolen from an employee's car. The bag contained the employee's computer and unencrypted backup media, which contained the names, addresses, dates of birth, Social Security numbers, insurance information and clinical information of approximately 55,000 current and former Cancer Care patients.

OCR's subsequent investigation found that, prior to the breach, Cancer Care was in widespread non-compliance with the HIPAA Security Rule. It had not conducted an enterprise-wide risk analysis when the breach occurred in July 2012. Further, Cancer Care did not have in place a written policy specific to the removal of hardware and electronic media containing ePHI into and out of its facilities, even though this was common practice within the organization. OCR found that these two issues, in particular, contributed to the breach, as an enterprise-wide risk analysis could have identified the removal of unencrypted backup media as an area of significant risk to Cancer Care's ePHI, and a comprehensive device and media control policy could have provided employees with direction regarding their responsibilities when removing devices containing ePHI from the facility.

In addition to the $750,000 settlement, the resolution agreement requires Cancer Care to:

- Conduct a comprehensive and thorough risk analyses of security risk and vulnerabilities;
- Develop an organization-wide risk management plan;
- Review and revise HIPAA Security Rule policies and procedures;
- Review and revise HIPAA Security Rule training program.

This settlement occurred in August of 2015.

Resolution Agreement with Lahey Hospital and Medical Center

Lahey Hospital and Medical Center (Lahey) agreed to settle potential violations of the HIPAA Privacy and Security Rules with OCR. Lahey paid $850,000 and agreed to adopt a robust corrective action plan to correct deficiencies in its HIPAA compliance program. Lahey is a non-profit teaching hospital affiliated with Tufts Medical School, providing primary and specialty care in Burlington, Massachusetts.

Lahey notified OCR that a laptop was stolen from an unlocked treatment room during the overnight hours on August 11, 2011. The laptop was on a stand that accompanied a portable CT scanner; the laptop operated the scanner and produced images for viewing through Lahey's Radiology Information System and Picture Archiving and Communication System. The laptop hard drive contained the PHI of 599 individuals. Evidence obtained through OCR's subsequent investigation indicated widespread non-compliance with the HIPAA rules, including:

- Failure to conduct a thorough risk analysis of all of its ePHI;
- Failure to physically safeguard a workstation that accessed ePHI;
- Failure to implement and maintain policies and procedures regarding the safeguarding of ePHI maintained on workstations utilized in connection with diagnostic/laboratory equipment;
- Lack of a unique user name for identifying and tracking user identity with respect to the workstation at issue in this incident;
- Failure to implement procedures that recorded and examined activity in the workstation at issue in this incident; and
- Impermissible disclosure of 599 individuals' PHI.

In addition to the $850,000 settlement, Lahey agreed to:

- Conduct a comprehensive and thorough risk analyses of security risk and vulnerabilities;
- Develop an organization-wide risk management plan; and
- Develop or revise as necessary written policies and procedures for device and media controls, workstation security, and audit controls.

This settlement occurred in November of 2015.

Resolution Agreement with Triple-S Management Corporation

Triple-S Management Corporation ("TRIPLE-S"), on behalf of its wholly owned subsidiaries, Triple-S Salud Inc., Triple-C Inc. and Triple-S Advantage Inc., formerly known as American Health Medicare Inc., agreed to settle potential violations of the HIPAA Privacy and Security Rules with OCR. TRIPLE-S paid $3.5 million and agreed to adopt a robust corrective action plan to correct deficiencies in its HIPAA compliance program, an effort it has already begun.

TRIPLE-S is an insurance holding company based in San Juan, Puerto Rico, which offers a wide range of insurance products and services to residents of Puerto Rico through its subsidiaries. TRIPLE-S cooperated with HHS in investigating this case and agreed to put in place a comprehensive HIPAA compliance program as a condition for settlement.

After receiving multiple breach notifications from TRIPLE-S involving unsecured PHI, OCR initiated investigations to ascertain the entities' compliance with HIPAA Rules. OCR's investigations indicated widespread non-compliance throughout the various subsidiaries of Triple-S, including:

- Failure to implement appropriate administrative, physical, and technical safeguards to protect the privacy of its beneficiaries' PHI;

- Impermissible disclosure of its beneficiaries' PHI to an outside vendor with which it did not have an appropriate business associate agreement;
- Use or disclosure of more PHI than was necessary to carry out mailings;
- Failure to conduct an accurate and thorough risk analysis that incorporates all IT equipment, applications, and data systems utilizing ePHI; and
- Failure to implement security measures sufficient to reduce the risks and vulnerabilities to its ePHI to a reasonable and appropriate level.

In addition to the $3.5 million settlement, TRIPLE-S agreed to:

- Conduct a comprehensive and thorough risk analyses of security risk and vulnerabilities;
- Develop an organization-wide risk management plan;
- Evaluate any environmental or operation changes that affect the security of ePHI;
- Review and revise as necessary HIPAA Privacy and Security Rule policies and procedures; and
- Train workforce members on revised HIPAA Privacy and Security Rule policies and procedures.

This settlement occurred in November of 2015.

Resolution Agreement with University of Washington Medicine

The University of Washington Medicine (UWM) agreed to settle potential violations of the HIPAA Security Rule with OCR. UWM paid $750,000 and agreed to adopt a robust corrective action plan to correct deficiencies in its HIPAA compliance program and provide annual reports on the organization's compliance efforts. UWM is an affiliated covered entity, which includes designated health care components and other entities under the control of the University of Washington, including University of Washington Medical Center, the primary teaching hospital of the University of Washington School of Medicine. Affiliated covered entities must have in place appropriate policies and processes to assure HIPAA compliance with respect to each of the entities that are part of the affiliated group.

The U.S. Department of Health and Human Services Office for Civil Rights (OCR) initiated its investigation of the UWM following receipt of a breach report on November 27, 2013, which indicated that the electronic protected health information (e-PHI) of approximately 90,000 individuals was accessed after an employee downloaded an email attachment that contained malicious malware. The malware compromised the organization's IT system, affecting the data of two different groups of patients: 1) approximately 76,000 patients involving a combination of patient names, medical record numbers, dates of service, and/or charges or bill balances; and 2) approximately 15,000 patients involving names, medical record numbers, other demographics such as address and phone number, dates of birth, charges or bill balances, social security numbers, insurance identification or Medicare numbers.

OCR's investigation indicated UWM's security policies required its affiliated entities to have up-to-date, documented system-level risk assessments and to implement safeguards in compliance

with the Security Rule. However, UWM did not ensure that all of its affiliated entities were properly conducting risk assessments and appropriately responding to the potential risks and vulnerabilities in their respective environments.

In addition to the $750,000 settlement, UWM agreed to:

- Conduct a comprehensive and thorough risk analyses of security risk and vulnerabilities; and
- Develop an organization-wide risk management plan.

This settlement occurred in December of 2015.

Resolution Agreement with North Memorial Health Care

North Memorial Health Care of Minnesota (North Memorial) paid $1.55 million to settle charges that it potentially violated the HIPAA Privacy and Security Rules by failing to enter into a business associate agreement with a major contractor and failing to institute an organization-wide risk analysis to address the risks and vulnerabilities to its patient information. North Memorial is a comprehensive, not-for-profit health care system in Minnesota that serves the Twin Cities and surrounding communities.

OCR initiated its investigation of North Memorial following receipt of a breach report on September 27, 2011, which indicated that an unencrypted, password-protected laptop was stolen from a business associate's workforce member's locked vehicle, impacting the ePHI of 9,497 individuals.

OCR's investigation indicated that North Memorial failed to have in place a business associate agreement, as required under the HIPAA Privacy and Security Rules, so that its business associate could perform certain payment and health care operations activities on its behalf. North Memorial gave its business associate, Accretive Health, Inc., access to North Memorial's hospital database, which stored the ePHI of 289,904 patients. Accretive also received access to non-electronic protected health information as it performed services on-site at North Memorial.

The investigation further determined that North Memorial failed to complete a risk analysis to address all of the potential risks and vulnerabilities to the ePHI that it maintained, accessed, or transmitted across its entire IT infrastructure -- including but not limited to all applications, software, databases, servers, workstations, mobile devices and electronic media, network administration and security devices, and associated business processes.

In addition to the $1.55 million settlement, North Memorial agreed to:

- Develop an organization-wide risk analysis and risk management plan; and
- Train appropriate workforce members on all policies and procedures newly developed or revised pursuant to its corrective action plan.

This settlement occurred in March of 2016.

Resolution Agreement with Feinstein Institute for Medical Research

Feinstein Institute for Medical Research (Feinstein) paid OCR $3.9 million to settle potential violations of the HIPAA Privacy and Security Rules and agreed to undertake a substantial corrective action plan to bring its operations into compliance. Feinstein is a biomedical research institute that is organized as a New York not-for-profit corporation and is sponsored by Northwell Health, Inc., formerly known as North Shore Long Island Jewish Health System, a large health system headquartered in Manhasset, New York that is comprised of twenty-one hospitals and over 450 patient facilities and physician practices.

OCR's investigation began after Feinstein filed a breach report indicating that on September 2, 2012, a laptop computer containing the ePHI of approximately 13,000 patients and research participants was stolen from an employee's car. The ePHI stored in the laptop included the names of research participants, dates of birth, addresses, social security numbers, diagnoses, laboratory results, medications, and medical information relating to potential participation in a research study.

OCR's investigation discovered that Feinstein's security management process was limited in scope, incomplete, and insufficient to address potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the entity. Further, Feinstein lacked policies and procedures for authorizing access to ePHI by its workforce members, failed to implement safeguards to restrict access to unauthorized users, and lacked policies and procedures to govern the receipt and removal of laptops that contained ePHI into and out of its facilities. For electronic equipment procured outside of Feinstein's standard acquisition process, Feinstein failed to implement proper mechanisms for safeguarding ePHI as required by the Security Rule.

In addition to the $3.9 million settlement, Feinstein agreed to:

- Develop an organization-wide risk analysis and risk management plan;
- Evaluate any environmental or operation changes that affect the security of ePHI; and
- Review and revise, if necessary, HIPAA Privacy and Security policies and procedures.

This settlement occurred in March of 2016.

Resolution Agreement with Raleigh Orthopaedic

Raleigh Orthopaedic Clinic, P.A. of North Carolina (Raleigh Orthopaedic) paid OCR $750,000 to settle charges that it potentially violated the HIPAA Privacy Rule by handing over PHI for approximately 17,300 patients to a potential business partner without first executing a business associate agreement. HIPAA covered entities cannot disclose PHI to unauthorized persons, and the lack of a business associate agreement left this sensitive health information without safeguards and vulnerable to misuse or improper disclosure. Raleigh Orthopaedic is a provider group practice that operates clinics and an orthopedic surgery center in the Raleigh, North Carolina area.

OCR initiated its investigation of Raleigh Orthopaedic following receipt of a breach report on April 30, 2013. OCR's investigation indicated that Raleigh Orthopaedic released the x-ray films and related protected health information of 17,300 patients to an entity that promised to transfer the images to electronic media in exchange for harvesting the silver from the x-ray films. Raleigh Orthopedic failed to execute a business associate agreement with this entity prior to turning over the x-rays (and PHI).

In addition to the $750,000 payment, Raleigh Orthopaedic is required to:

- Revise its policies and procedures;
- Establish a process for assessing whether entities are business associates;
- Designate a responsible individual to ensure business associate agreements are in place prior to disclosing PHI to a business associate;
- Create a standard template business associate agreement;
- Establish a standard process for maintaining documentation of a business associate agreements for at least six (6) years beyond the date of termination of a business associate relationship; and
- Limit disclosures of PHI to any business associate to the minimum necessary to accomplish the purpose for which the business associate was hired.

This settlement occurred in April of 2016.

Resolution Agreement with Catholic Health Care Services of the Archdiocese of Pennsylvania

Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS) agreed to settle potential violations of the HIPAA Security Rule after the theft of a CHCS mobile device compromised the PHI of hundreds of nursing home residents. CHCS provided management and information technology services as a business associate to six skilled nursing facilities. The total number of individuals affected by the combined breaches was 412. The settlement includes a monetary payment of $650,000 and a corrective action plan.

OCR initiated its investigation on April 17, 2014, after receiving notification that CHCS had experienced a breach of PHI involving the theft of a CHCS-issued employee iPhone. The iPhone was unencrypted and was not password protected. The information on the iPhone was extensive, and included social security numbers, information regarding diagnosis and treatment, medical procedures, names of family members and legal guardians, and medication information. At the time of the incident, CHCS had no policies addressing the removal of mobile devices containing PHI from its facility or what to do in the event of a security incident; OCR also determined that CHCS had no risk analysis or risk management plan.

In determining the resolution amount, OCR considered that CHCS provides unique and much-needed services in the Philadelphia region to the elderly, developmentally disabled individuals, young adults aging out of foster care, and individuals living with HIV/AIDS.

OCR will monitor CHCS for two years as part of this settlement agreement, helping ensure that CHCS will remain compliant with its HIPAA obligations while it continues to act as a Business Associate.

In addition to the $650,000 settlement, CHCS agreed to:

- Develop an organization-wide risk analysis and risk management plan;
- Develop, maintain, review and revise, if necessary, Security Policies and Procedures; and
- Provide documentation of all business associate agreements where CHCS acts as a business associate to a covered entity; and
- Train workforce members on HIPAA Security Rule policies and procedures.

This settlement occurred in June of 2016.

Resolution Agreement with Oregon Health and Science University

Oregon Health & Science University (OHSU) agreed to settle potential violations of the HIPAA Privacy and Security Rules following an investigation by OCR that found widespread and diverse problems at OHSU, which will be addressed through a comprehensive three-year corrective action plan. The settlement included a monetary payment by OHSU to the Department for $2.7 million.

OCR's investigation began after OHSU submitted multiple breach reports affecting thousands of individuals, including two reports involving unencrypted laptops and another large breach involving a stolen unencrypted thumb drive. These incidents each garnered significant local and national press coverage. OCR's investigation uncovered evidence of widespread vulnerabilities within OHSU's HIPAA compliance program, including the storage of the ePHI of over 3,000 individuals on a cloud-based server without a business associate agreement. OCR found significant risk of harm to 1,361 of these individuals due to the sensitive nature of their diagnoses. The server stored a variety of ePHI including credit card and payment information, diagnoses, procedures, photos, driver's license numbers and Social Security numbers.

OHSU performed risk analyses in 2003, 2005, 2006, 2008, 2010, and 2013, but OCR's investigation found that these analyses did not cover all ePHI in OHSU's enterprise, as required by the Security Rule. While the analyses identified vulnerabilities and risks to ePHI located in many areas of the organization, OHSU did not act in a timely manner to implement measures to address these documented risks and vulnerabilities. OHSU also lacked policies and procedures to prevent, detect, contain, and correct security violations and failed to implement a mechanism to encrypt and decrypt ePHI or an equivalent alternative measure for ePHI maintained on its workstations, despite having identified this lack of encryption as a risk.

OHSU is a large public academic health center and research university centered in Portland, Oregon, comprising two hospitals, and multiple general and specialty clinics throughout Portland and throughout the State of Oregon.

In addition to the $2.7 million settlement agreement, OHSU agreed to:

- Develop an organization-wide risk analysis and risk management plan;

- Provide update on encryption status including a mobile device management solution and status for laptops, desktops and medical equipment; and
- Provide security awareness training to workforce members.

This settlement occurred in July of 2016.

Resolution Agreement with University of Mississippi Medical Center

The University of Mississippi (UM) Medical Center (UMMC) agreed to settle multiple alleged violations of HIPAA with OCR. During the investigation, OCR determined that UMMC was aware of risks and vulnerabilities to its systems as far back as April 2005, yet no significant risk management activity occurred until after the breach, due largely to organizational deficiencies and insufficient institutional oversight. UMMC paid a $2.75 million and agreed to adopt a corrective action plan to help assure future compliance with HIPAA Privacy, Security, and Breach Notification Rules.

On March 21, 2013, OCR was notified of a breach, after UMMC's privacy officer discovered that a password-protected laptop was missing from UMMC's Medical Intensive Care Unit (MICU). UMMC's investigation concluded that it had likely been stolen by a visitor to the MICU who had inquired about borrowing one of the laptops. OCR's investigation revealed that ePHI stored on a UMMC network drive was vulnerable to unauthorized access via UMMC's wireless network, because users could access an active directory containing 67,000 files after entering a generic username and password. The directory included 328 files containing the ePHI of an estimated 10,000 patients dating back to 2008.

Further, OCR's investigation revealed that UMMC:

- Failed to implement appropriate policies and procedures to prevent, detect, contain, and correct security violations;
- Failed to implement physical safeguards for all workstations that access ePHI to restrict access to authorized users;
- Failed to assign a unique user name and/or number for identifying and tracking user identity in information systems containing ePHI; and
- Failed to notify each individual whose unsecured ePHI was reasonably believed to have been accessed, acquired, used, or disclosed as a result of the breach.

UM is Mississippi's sole public academic health science center, with education and research functions in addition to providing patient care in four specialized hospitals on the Jackson campus and at clinics throughout Jackson and the State. Its designated health care component, UMMC, includes University Hospital, the site of the breach in this case, located on the main UMMC campus in Jackson.

In addition to the $2.75 million settlement, UMMC agreed to:

- Designate an internal monitor to review UMMC's compliance with corrective action plan;

- Develop an organization-wide risk analysis and risk management plan;
- Update Security Rule policies and procedures;
- Revise Breach Notification Policies;
- Develop plan to implement unique user identification; and
- Provide security awareness training to workforce members.

This settlement occurred in July of 2016.

Resolution Agreement with Advocate Health Care Network

Advocate Health Care Network (Advocate) agreed to a settlement with OCR, for multiple potential violations of HIPAA involving ePHI. Advocate paid $5.55 million and agreed to adopt a corrective action plan. This significant settlement, the largest to-date against a single entity, was a result of the extent and duration of the alleged noncompliance (dating back to the inception of the Security Rule in some instances), the involvement of the State Attorney General in a corresponding investigation, and the large number of individuals whose information was affected by Advocate, one of the largest health systems in the country.

OCR began its investigation in 2013, when Advocate submitted three breach notification reports pertaining to separate and distinct incidents involving its subsidiary, Advocate Medical Group ("AMG"). The combined breaches affected the ePHI of approximately 4 million individuals. The ePHI included demographic information, clinical information, health insurance information, patient names, addresses, credit card numbers and their expiration dates, and dates of birth. OCR's investigations into these incidents revealed that Advocate:

- Failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to all of its ePHI;
- Failed to implement policies and procedures and facility access controls to limit physical access to the electronic information systems housed within a large data support center;
- Failed to obtain satisfactory assurances in the form of a written business associate contract that its business associate would appropriately safeguard all ePHI in its possession; and
- Failed to reasonably safeguard an unencrypted laptop when left in an unlocked vehicle overnight.

Advocate Health Care Network is the largest fully integrated health care system in Illinois, with more than 250 treatment locations, including ten acute-care hospitals and two integrated children's hospitals. Its subsidiary, AMG, is a non-profit physician-led medical group that provides primary care, medical imaging, outpatient and specialty services throughout the Chicago area and in Bloomington-Normal, Illinois.

In addition to the $5.55 million settlement, Advocate agreed to:

- Conduct a comprehensive and thorough risk analyses of security risk and vulnerabilities;
- Develop an enterprise-wide risk management plan;
- Evaluate any environmental or operation changes that affect the security of ePHI;

- Develop an encryption report regarding status of all devices and equipment that may be used to access, store, download or transmit ePHI;
- Review and revise policies and procedures on device and media controls; facility access controls; and business associates; and
- Develop enhanced Privacy and Security Awareness Training.

This settlement occurred in August of 2016.

Resolution Agreement with Care New England Health System (Women and Infants Hospital)

Care New England Health System (CNE), on behalf of each of the covered entities under its common ownership or control, agreed to settle potential violations of the HIPAA Privacy and Security Rules. The settlement included a monetary payment of $400,000 and a comprehensive corrective action plan. CNE provides centralized corporate support for its subsidiary affiliated covered entities, which include a number of hospitals and health care providers in Massachusetts and Rhode Island. These functions include, but are not limited to, finance, human resources, information services and technical support, insurance, compliance and administrative functions.

On November 5, 2012, OCR received notification from Woman & Infants Hospital of Rhode Island (WIH), a covered entity member of CNE, of the loss of unencrypted backup tapes containing the ultrasound studies of approximately 14,000 individuals, including patient name, date of birth, date of exam, physician names, and, in some instances, Social Security Numbers. As WIH's business associate, CNE provides centralized corporate support including technical support and information security for WIH's information systems. WIH provided OCR with a business associate agreement with Care New England Health System effective March 15, 2005, that was not updated until August 28, 2015, as a result of OCR's investigation, and therefore, did not incorporate revisions required under the 2013 HIPAA Omnibus Final Rule.

OCR's investigation found the following:

- From September 23, 2014 until August 28, 2015, WIH disclosed PHI and allowed its business associate, CNE, to create, receive, maintain, or transmit PHI on its behalf, without obtaining satisfactory assurances as required under HIPAA. WIH failed to renew or modify its existing written business associate agreement with CNE to include the applicable implementation specifications required by the HIPAA Privacy and Security Rules.
- From September 23, 2014, until August 28, 2015, WIH impermissibly disclosed the PHI of at least 14,004 individuals to its business associate when WIH provided CNE with access to PHI without obtaining satisfactory assurances, in the form of a written business associate agreement, that CNE would appropriately safeguard the PHI.

With respect to the underlying breach, on July 17, 2014, WIH entered into a consent judgment with the Massachusetts Attorney General's Office (AGO), and reached a settlement of $150,000. OCR found the consent judgment to sufficiently cover most of the conduct in this breach, including the failure to implement appropriate safeguards related to the handling of the PHI contained on the backup tapes and the failure to provide timely notification to the affected individuals. While the AGO's actions do not legally preclude OCR from imposing civil money penalties, OCR determined not to include additional potential violations in this case for the

purposes of settlement, given that such potential violations had already been addressed by the AGO and based on OCR's policy approach to concurrent cases with State AGOs.

In addition to the $400,000 settlement, CNE agreed to:

- Review and revise, if necessary, HIPAA Privacy and Security Policies and Procedures; and
- Train workforce members on HIPAA Privacy and Security Rule Policies and Procedures.

This settlement occurred in September of 2016.

Resolution Agreement with St. Joseph Health Ministry

St. Joseph Health Ministry (SJH) agreed to settle potential violations of the HIPAA Privacy and Security Rules following the report that files containing ePHI were publicly accessible through internet search engines from 2011 until 2012. SJH, a non-profit integrated Catholic health care delivery system sponsored by the St. Joseph Health Ministry, paid a settlement amount of $2.14 million and agreed to adopt a comprehensive corrective action plan. SJH's range of services includes 14 acute care hospitals, home health agencies, hospice care, outpatient services, skilled nursing facilities, community clinics and physician organizations throughout California and in parts of Texas and New Mexico.

On February 14, 2012, SJH reported OCR that certain files it created for its participation in the meaningful use program, which contained ePHI, were publicly accessible on the internet from February 1, 2011, until February 13, 2012, via Google and possibly other internet search engines. The server SJH purchased to store the files included a file sharing application whose default settings allowed anyone with an internet connection to access them. Upon implementation of this server and the file sharing application, SJH did not examine or modify it. As a result, the public had unrestricted access to PDF files containing the ePHI of 31,800 individuals, including patient names, health statuses, diagnoses, and demographic information.

OCR's investigation indicated the following potential violations of the HIPAA Rules:

- SJH potentially disclosed the PHI of 31,800 individuals;
- Evidence indicated that SJH failed to conduct an evaluation in response to the environmental and operational changes presented by implementation of a new server for its meaningful use project, thereby compromising the security of ePHI; and
- Although SJH hired a number of contractors to assess the risks and vulnerabilities to the confidentiality, integrity and availability of ePHI held by SJH, evidence indicated that this was conducted in a patchwork fashion and did not result in an enterprise-wide risk analysis, as required by the HIPAA Security Rule.

In addition to the $2.14 million settlement, SJH agreed to:

- Conduct a comprehensive and thorough risk analyses of security risk and vulnerabilities;
- Develop and implement a risk management plan;
- Revise its use and disclosure of protected health information policies and procedures; and

- Train its staff on these revised policies and procedures.

This settlement occurred in October of 2016.

Resolution Agreement with University of Massachusetts Amherst

The University of Massachusetts Amherst (UMass) agreed to settle potential violations of the HIPAA Privacy and Security Rules. The settlement includes a corrective action plan and a monetary payment of $650,000, which is reflective of the fact that the University operated at a financial loss in 2015.

On June 18, 2013, UMass reported to OCR that a workstation in its Center for Language, Speech, and Hearing (the "Center") was infected with a malware program, which resulted in the impermissible disclosure of ePHI of 1,670 individuals, including names, addresses, Social Security numbers, dates of birth, health insurance information, diagnoses and procedure codes. The University determined that the malware was a generic remote access Trojan that infiltrated their system, providing impermissible access to ePHI, because UMass did not have a firewall in place.

OCR's investigation indicated the following potential violations of the HIPAA Rules:

- UMass had failed to designate all of its health care components when hybridizing, incorrectly determining that while its University Health Services was a covered health care component, other components, including the Center where the breach of ePHI occurred, were not covered components. Because UMass failed to designate the Center a health care component, UMass did not implement policies and procedures at the Center to ensure compliance with the HIPAA Privacy and Security Rules. (Note: The HIPAA Privacy Rule permits legal entities that have some functions that are covered by HIPAA and some that are not to elect to become a "hybrid entity." To successfully "hybridize," the entity must designate in writing the health care components that perform functions covered by HIPAA and assure HIPAA compliance for its covered health care components.)
- UMass failed to implement technical security measures at the Center to guard against unauthorized access to ePHI transmitted over an electronic communications network by ensuring that firewalls were in place at the Center.
- Finally, UMass did not conduct an accurate and thorough risk analysis until September 2015.

In addition to the monetary settlement, UMass agreed to a corrective action plan that requires the organization to:

- Conduct an enterprise-wide risk analysis;
- Develop and implement a risk management plan;
- Revise its policies and procedures for the HIPAA Privacy Rule and Breach Notification Rule; and
- Train its staff on these revised policies and procedures.

This settlement occurred in November of 2016.

Resolution Agreement with Presence Health

Presence Health agreed to settle potential violations of the HIPAA Breach Notification Rule with OCR. Presence paid $475,000 and agreed to adopt a corrective action plan to correct deficiencies in its HIPAA compliance program. Presence Health is one of the largest health care networks serving Illinois and consists of approximately 150 locations, including 11 hospitals and 27 long-term care and senior living facilities. Presence also has multiple physicians' offices and health care centers in its system and offers home care, hospice care, and behavioral health services.

On January 31, 2014, OCR received a breach notification report from Presence indicating that on October 22, 2013, Presence discovered that paper-based operating room schedules, which contained the PHI of 836 individuals, were missing from the Presence Surgery Center at the Presence St. Joseph Medical Center in Joliet, Illinois. The information consisted of the affected individuals' names, dates of birth, medical record numbers, dates of procedures, types of procedures, surgeon names, and types of anesthesia. OCR's investigation revealed that Presence Health failed to notify, without unreasonable delay and within 60 days of discovering the breach, each of the 836 individuals affected by the breach, prominent media outlets (as required for breaches affecting 500 or more individuals), and OCR.

In addition to the $475,000 settlement amount, the agreement requires Presence to:

- To revise its policies and procedures to comply with the Breach Notification Rule;
- Explicitly delineate its workforce members roles and responsibilities for receiving and addressing internal and external reports involving the potential breach of PHI;
- Train its workforce members; and
- To revise its policies for sanctioning employees who fail to comply with its policies and procedures for implementing the Breach Notification Rule.

This settlement occurred in January of 2017.

Resolution Agreement with MAPFRE Life Insurance Company

MAPFRE Life Insurance Company of Puerto Rico (MAPFRE) agreed to settle potential noncompliance with the HIPAA Privacy and Security Rules with OCR. MAPFRE paid $2.2 million and agreed to adopt a corrective action plan to correct deficiencies with its HIPAA compliance program. MAPFRE is a subsidiary company of MAPFRE S.A., a global multinational insurance company headquartered in Spain. MAPFRE underwrites and administers a variety of insurance products and services in Puerto Rico, including personal and group health insurance plans.

On September 29, 2011, MAPFRE filed a breach report with OCR indicating that a USB data storage device containing ePHI was stolen from its IT department, where the device was left without safeguards. According to the report, the USB data storage device included complete

names, dates of birth and Social Security numbers. The report noted that the breach affected 2,209 individuals. MAPFRE informed OCR that it was able to identify the breached ePHI by reconstituting the data on the computer on which the USB data storage device was attached.

OCR's investigation revealed MAPFRE's noncompliance with the HIPAA Rules, specifically a failure to conduct its risk analysis and implement risk management plans, contrary to its prior representations. In addition, MAPFRE failed to deploy encryption or an equivalent alternative measure on its laptops and removable storage media until September 1, 2014. MAPFRE also failed to implement or delayed implementing other corrective measures it informed OCR it would undertake. In addition to the $2.2 million settlement amount, the agreement requires MAPFRE to:

- Develop a comprehensive corrective action plan;
- Conduct a thorough risk analysis and implement a risk management plan; and
- Train its workforce members.

This settlement occurred in January 2017.

Civil Money Penalty involving Children's Medical Center of Dallas

Children's Medical Center of Dallas (Children's) impermissibly disclosed electronic protected health information (ePHI) and was found to be in non-compliance with multiple standards of the HIPAA Security Rule. OCR issued a Notice of Proposed Determination in accordance with 45 CFR 160.420, which included instruction for how Children's could file a request for a hearing. Children's did not request a hearing. Accordingly, OCR issued a Notice of Final Determination and Children's paid the full civil money penalty of $3.2 million. Children's is a pediatric hospital in Dallas, Texas, and is part of Children's Health, the seventh largest pediatric health care provider in the nation.

On January 18, 2010, Children's filed a breach report with OCR indicating the loss of an unencrypted, non-password protected BlackBerry device at the Dallas/Fort Worth International Airport on November 19, 2009. The device contained the ePHI of approximately 3,800 individuals. On July 5, 2013, Children's filed a separate HIPAA Breach Notification Report with OCR, reporting the theft of an unencrypted laptop from its premises sometime between April 4 and April 9, 2013. Children's reported that the device contained the ePHI of 2,462 individuals. Although Children's implemented some physical safeguards to the laptop storage area (e.g., badge access and a security camera at one of the entrances), it also provided access to the area to workforce not authorized to access ePHI.

OCR's investigation revealed Children's noncompliance with HIPAA Rules, specifically, a failure to implement risk management plans, contrary to prior external recommendations to do so, and a failure to deploy encryption or an equivalent alternative measure on all of its laptops, work stations, mobile devices and removable storage media until April 9, 2013. Despite Children's knowledge about the risk of maintaining unencrypted ePHI on its devices as far back as 2007, Children's issued unencrypted BlackBerry devices to nurses and allowed its workforce members to continue using unencrypted laptops and other mobile devices until 2013.

This civil money penalty was imposed in January of 2017.

Resolution Agreement with Memorial Healthcare System

Memorial Healthcare System (MHS) paid $5.5 million to settle potential violations of the HIPAA Privacy and Security Rules with OCR. MHS agreed to adopt a corrective action plan. MHS is a nonprofit corporation which operates six hospitals, an urgent care center, a nursing home, and a variety of ancillary health care facilities throughout the South Florida area. MHS is also affiliated with physician offices through an Organized Health Care Arrangement (OHCA).

MHS reported to OCR that the protected health information (PHI) of 115,143 individuals had been impermissibly accessed by its employees and impermissibly disclosed to affiliated physician office staff. This information consisted of the affected individuals' names, dates of birth, and Social Security numbers. The login credentials of a former employee of an affiliated physician's office had been used to access the ePHI maintained by MHS on a daily basis without detection from April 2011 to April 2012, affecting 80,000 individuals. Although it had workforce access policies and procedures in place, MHS failed to implement procedures with respect to reviewing, modifying and/or terminating users' right of access, as required by the HIPAA Rules. Further, MHS failed to regularly review records of information system activity on applications that maintain electronic protected health information by workforce users and users at affiliated physician practices, despite having identified this risk on several risk analyses conducted by MHS from 2007 to 2012.

In addition to the $5,500,000 settlement amount, MHS must complete a risk analysis and risk management plan that includes:

- All identified risks and vulnerabilities identified at MHS related to enterprise-wide PHI security;
- Evidence that MHS has implemented and maintains a risk management plan to address such risks and vulnerabilities and expected dates of implementation; and
- Revision of its policies and procedures regarding information system activity review which requires the regular review of audit logs, access reports, and security incident tracking reports. In addition, the policies and procedures will address computer system access establishment, modification and termination.

This settlement occurred in February of 2017.

Resolution Agreement with Metro Community Provider Network

Metro Community Provider Network (MCPN) agreed to settle charges that it potentially violated the HIPAA Security Rules based on the lack of a security management process to safeguard electronic protected health information (ePHI). Metro Community Provider Network (MCPN), a federally-qualified health center (FQHC). MCPN provides primary medical care, dental care, pharmacies, social work, and behavioral health care services throughout the greater Denver, Colorado metropolitan area to approximately 43,000 patients per year, a large majority of whom have incomes at or below the poverty level.

On January 27, 2012, MCPN filed a breach report with OCR indicating that a hacker accessed employees' email accounts and obtained 3,200 individuals' ePHI through a phishing incident. OCR's investigation revealed that MCPN took necessary corrective action related to the phishing incident; however, the investigation also revealed that MCPN failed to conduct a risk analysis until mid-February 2012. Prior to the breach incident, MCPN had not conducted a risk analysis to assess the risks and vulnerabilities in its ePHI environment, and, consequently, had not implemented any corresponding risk management plans to address the risks and vulnerabilities identified in a risk analysis. When MCPN finally conducted a risk analysis, that risk analysis, as well as all subsequent risk analyses, were insufficient to meet the requirements of the Security Rule.

In addition to the $400,000 settlement amount, the agreement requires MCPN to:

- Develop a comprehensive corrective action plan;
- Conduct a thorough risk analysis and implement a risk management plan; and
- Train its workforce members.

This settlement occurred in April of 2017.

Resolution Agreement with the Center for Children's Digestive Health

The Center for Children's Digestive Health (CCDH) agreed to settle potential violations of the HIPAA Privacy Rule with OCR. CCDH is a small, for-profit health care provider with a pediatric subspecialty practice that operates its practice in seven clinic locations in Illinois.

In August 2015, OCR initiated a compliance review of the Center for Children's Digestive Health (CCDH), following an initiation of an investigation of a business associate, FileFax, Inc., which stored records containing protected health information (PHI) for CCDH. While CCDH began disclosing PHI to Filefax in 2003, neither party could produce a signed Business Associate Agreement (BAA) prior to Oct. 12, 2015.

In addition to the $31,000 settlement amount, the agreement requires CCDH to:

- Develop and implement a corrective action plan to address HIPAA Privacy Rule requirements regarding the contents and requirements of business associate agreements;
- Revise its policies and procedures; and
- Train its workforce members.

This settlement occurred in April of 2017.

Resolution Agreement with CardioNet

CardioNet agreed to settle potential violations of the HIPAA Privacy and Security Rules with OCR. CardioNet impermissibly disclosed the unsecured electronic protected health information (ePHI) of 1,391 individuals. This settlement is the first involving a wireless health services

provider, as CardioNet provides remote mobile monitoring of and rapid response to patients at risk for cardiac arrhythmias.

In January 2012, CardioNet reported to OCR that a workforce member's laptop was stolen from a parked vehicle outside of the employee's home. The laptop contained the ePHI of 1,391 individuals. OCR's investigation into the impermissible disclosure revealed that CardioNet had an insufficient risk analysis and risk management processes in place at the time of the theft. Additionally, CardioNet's policies and procedures implementing the standards of the HIPAA Security Rule were in draft form and had not been implemented. Further, the Pennsylvania-based organization was unable to produce any final policies or procedures regarding the implementation of safeguards for ePHI, including those for mobile devices.

In addition to the $2.5 million settlement amount, the agreement requires CardioNet to:

- Develop a corrective action plan an conduct a risk analysis of security risks, threats, and vulnerabilities enterprise-wide;
- Revise its policies and procedures governing the removal of hardware and electronic media into and outside of its facilities as well as the encryption of hardware and electronic media;
- Revise its training materials; and
- Train its workforce members.

This settlement occurred in April of 2017.

Resolution Agreement with Memorial Hermann Health System

Memorial Hermann Health System (MHHS) agreed to pay $2.4 million to settle potential violations of the HIPAA Privacy Rule with OCR. MHHS is a not-for-profit health system located in Southeast Texas, comprised of 16 hospitals and specialty services in the Greater Houston area.

The HHS Office for Civil Rights (OCR) initiated a compliance review of MHHS based on multiple media reports suggesting that MHHS disclosed a patient's protected health information (PHI) without an authorization. In September 2015, a patient at one of MHHS's clinics presented an allegedly fraudulent identification card to office staff. The staff immediately alerted appropriate authorities of the incident, and the patient was arrested. This disclosure of PHI to law enforcement was permitted under the HIPAA Rules. However, MHHS subsequently published a press release concerning the incident in which MHHS senior management approved the impermissible disclosure of the patient's PHI by adding the patient's name in the title of the press release. In addition, MHHS failed to timely document the sanctioning of its workforce members for impermissibly disclosing the patient's information.

In addition to a $2.4 million monetary settlement, a corrective action plan requires MHHS to update its policies and procedures on safeguarding PHI from impermissible uses and disclosures and to train its workforce members. The corrective action plan also requires all MHHS facilities

to attest to their understanding of permissible uses and disclosures of PHI, including disclosures to the media.

This settlement occurred in April of 2017.

Resolution Agreement with St. Luke's – Roosevelt Hospital Center

St. Luke's-Roosevelt Hospital Center Inc. (St. Luke's) paid OCR $387,200 to settle potential violations of the HIPAA Privacy Rule and agreed to implement a comprehensive corrective action plan. St. Luke's operates the Institute for Advanced Medicine, formerly Spencer Cox Center for Health (the Spencer Cox Center), which provides comprehensive health services to persons living with HIV or AIDS and other chronic diseases. St. Luke's is 1 of 7 hospitals that comprise the Mount Sinai Health System (MSHS).

In September 2014, the HHS Office for Civil Rights (OCR) received a complaint alleging that a staff member from the Spencer Cox Center impermissibly disclosed the complainant's protected health information (PHI) to the complainant's employer. This impermissible disclosure included sensitive information concerning HIV status, medical care, sexually transmitted diseases, medications, sexual orientation, mental health diagnosis, and physical abuse. OCR's subsequent investigation revealed that staff at the Spencer Cox Center impermissibly faxed the patient's PHI to his employer rather than sending it to the requested personal post office box. Additionally, OCR discovered that the Spencer Cox Center was responsible for a related breach of sensitive information that occurred nine months prior to the aforementioned incident, but had not addressed the vulnerabilities in their compliance program to prevent impermissible disclosures.

In addition to the settlement amount, St. Luke's agreed to:

- Develop a corrective action plan to address the release of protected health information;
- Revise its policies and procedures regarding the uses and disclosures of protected health information; and
- Update its training materials and train its workforce members.

This settlement occurred in May of 2017.

Resolution Agreement with 21st Century Oncology

21st Century Oncology, Inc. (21CO) agreed to pay $2.3 million in lieu of potential civil money penalties to OCR to settle potential violations of the HIPAA Privacy and Security Rules. 21CO is a provider of cancer care services and radiation oncology. With their headquarters located in Fort Myers, Florida, 21CO operates and manages 179 treatment centers, including 143 centers located in 17 states and 36 centers located in seven countries in Latin America.

On two separate occasions in 2015, the Federal Bureau of Investigation (FBI) notified 21CO that patient information was illegally obtained by an unauthorized third party and produced 21CO patient files purchased by an FBI informant. As part of its internal investigation, 21CO determined that the attacker may have accessed 21CO's network SQL database as early as October 3, 2015, through the remote desktop protocol from an exchange server within 21CO's

network. 21CO determined that 2,213,597 individuals were affected by the impermissible access to their names, Social Security numbers, physicians' names, diagnoses, treatment, and insurance information. OCR's subsequent investigation revealed that 21CO failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the electronic protected health information (ePHI); failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level; failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports; and disclosed protected health information (PHI) to third party vendors without a written business associate agreement.

In addition to the $2.3 million monetary settlement, a corrective action plan requires 21CO to:

- Complete a risk analysis and risk management plan to assess threats and mitigate harm involving risks and vulnerabilities among its information systems;
- Revise policies and procedures;
- Educate its workforce members on revised policies and procedures;
- Provide all maintained business associate agreements to OCR; and
- Submit an internal monitoring plan to OCR.

This settlement occurred in December of 2017.

On May 25, 2017, 21CO filed for Chapter 11 bankruptcy protection in the United States Bankruptcy Court for the Southern District of New York. The settlement with OCR will resolve OCR's claims against 21CO and the corrective action plan will ensure that the reorganized entity emerges from bankruptcy with a strong HIPAA compliance program in place. The settlement with OCR was approved by the Bankruptcy Court on December 11, 2017.