Annual Report to Congress on Breaches of Unsecured Protected Health Information

For Calendar Year 2018

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 year 2018.[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 of unsecured PHI. Section 13402(h) of the HITECH Act defines "unsecured protected health information" as "protected health information that is not secured through the use of a technology or methodology specified by the Secretary in guidance" and 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 updated 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 such 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] All previous Reports to Congress are available on OCR's website: https://www.hhs.gov/hipaa/for-professionals/breach-notification/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 are set forth 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 received 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 an unauthorized person to whom the 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 the media, as applicable, on behalf of the covered entity.

- **Individual Notice**

Covered entities must notify affected individuals of a breach of unsecured PHI without unreasonable delay and no 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 no later than 60 calendar 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). If a breach involves fewer than 500 individuals, the covered entity it may submit a report(s) of such breach(es) 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, 2018, and December 31, 2018, and describes actions that have been taken by covered entities and business associates in response to these breaches.

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 the Calendar Year of 2018. OCR opens compliance reviews to investigate all reported breaches affecting 500 or more individuals, and may open compliance reviews into 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 2018, the Department entered into five resolution agreements/corrective action plans or imposed civil money penalties totaling more than $27.3 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 302 reports of such

breaches for calendar year 2018,[4] which affected a total of approximately 12,196,601 individuals.[5]

Breaches in 2018 Affecting 500 or More Individuals[6]

For the 302 breaches affecting 500 or more individuals in 2018, OCR received:

(1) 224 reports (74%) of breaches from health care providers (affecting 4,002,947 individuals (33%));
(2) 46 reports (15%) of breaches from health plans (affecting 2,745,432 individuals (22%)); and
(3) 32 reports (11%) of breaches from business associates (affecting 5,448,222 individuals (45%)).

See Figures 1 and 2.

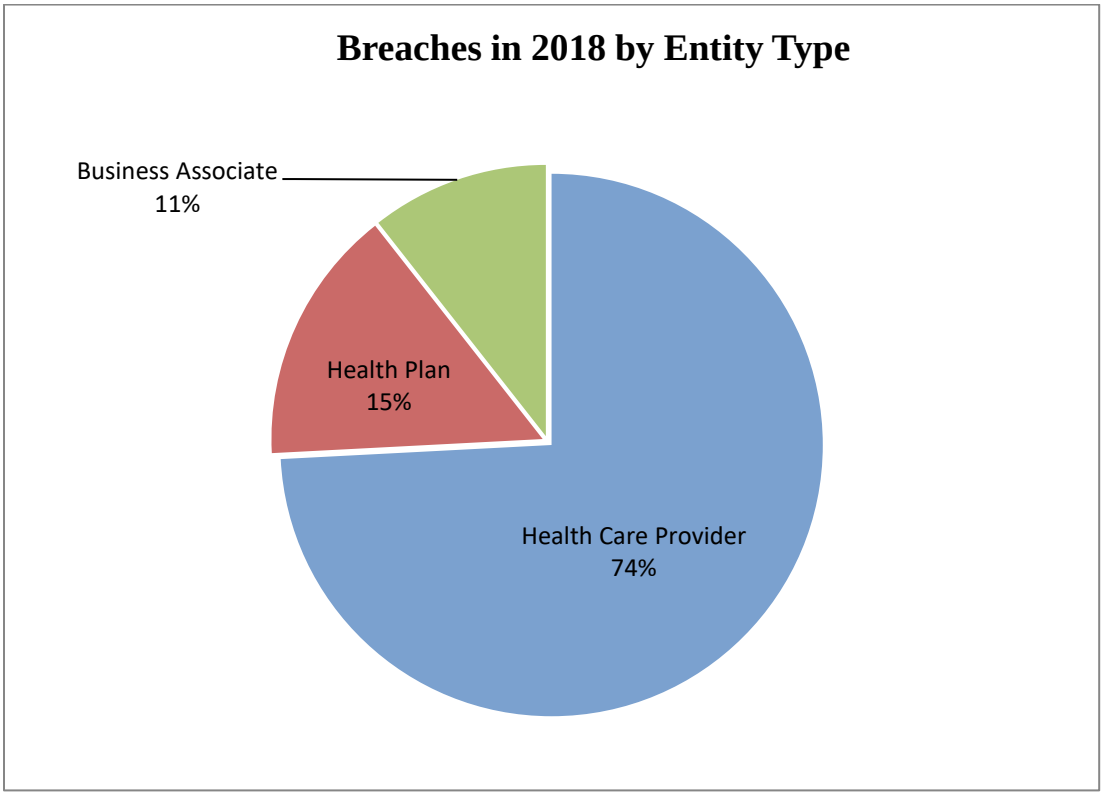

Figure 1

[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 2016 into 2018 would be reported with the 2018 figures.
[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.

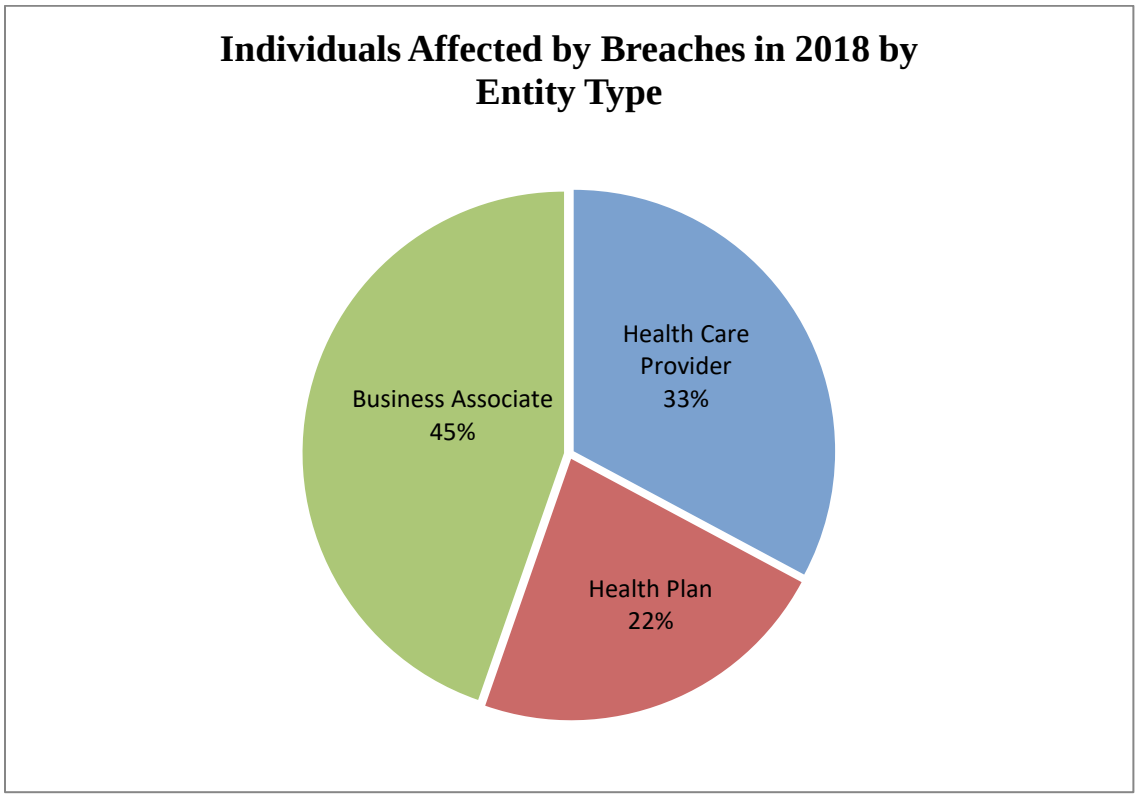

Figure 2

The 302 reports submitted to OCR for breaches affecting 500 or more individuals occurring in 2018 can be categorized by five general causes as follows (in order of frequency):

(1) Hacking/IT incident of electronic equipment or a network server (126 reports (42%) affecting 8,140,341 individuals (67%));
(2) Unauthorized access or disclosure of records containing PHI (123 reports (41%) affecting 3,018,241 individuals (25%));
(3) Theft of electronic equipment/portable devices or paper containing PHI (39 reports (13%), affecting 685,565 individuals (6%));
(4) Loss of electronic media or paper records containing PHI (7 reports (2%) affecting 14,269 individuals (<1%)); and
(5) Improper disposal of PHI (7 reports (2%) affecting 338,185 individuals (3%)).

See Figures 3 and 4.

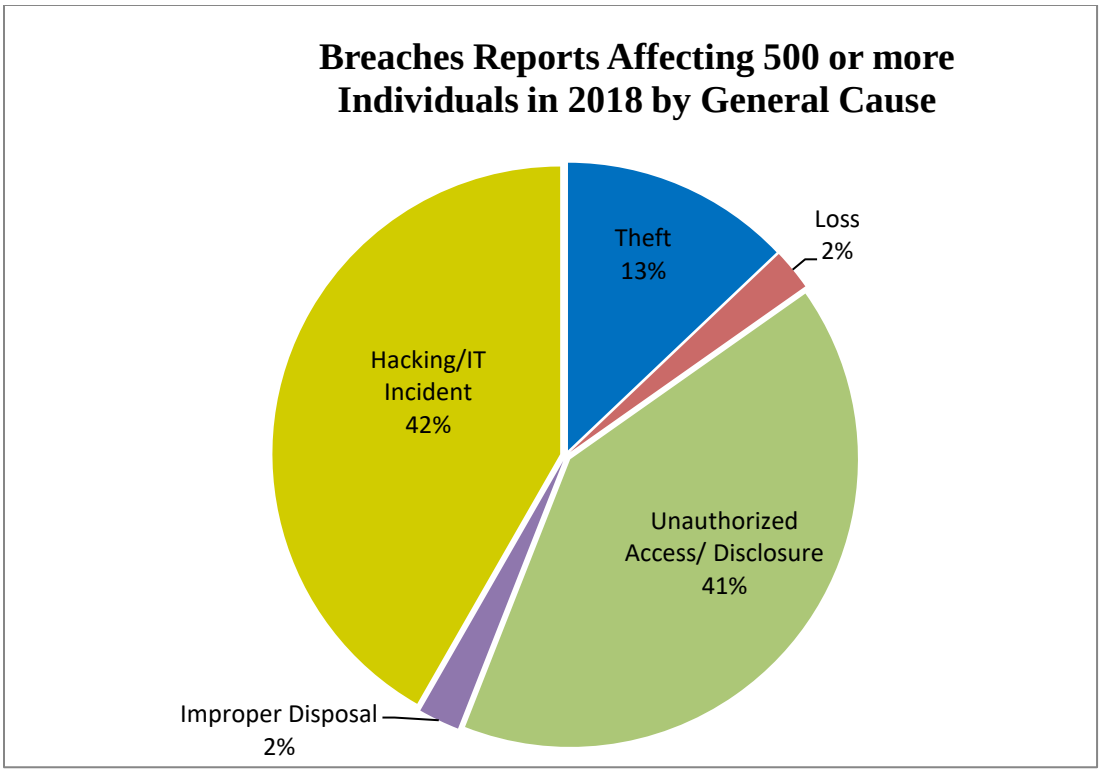

Figure 3

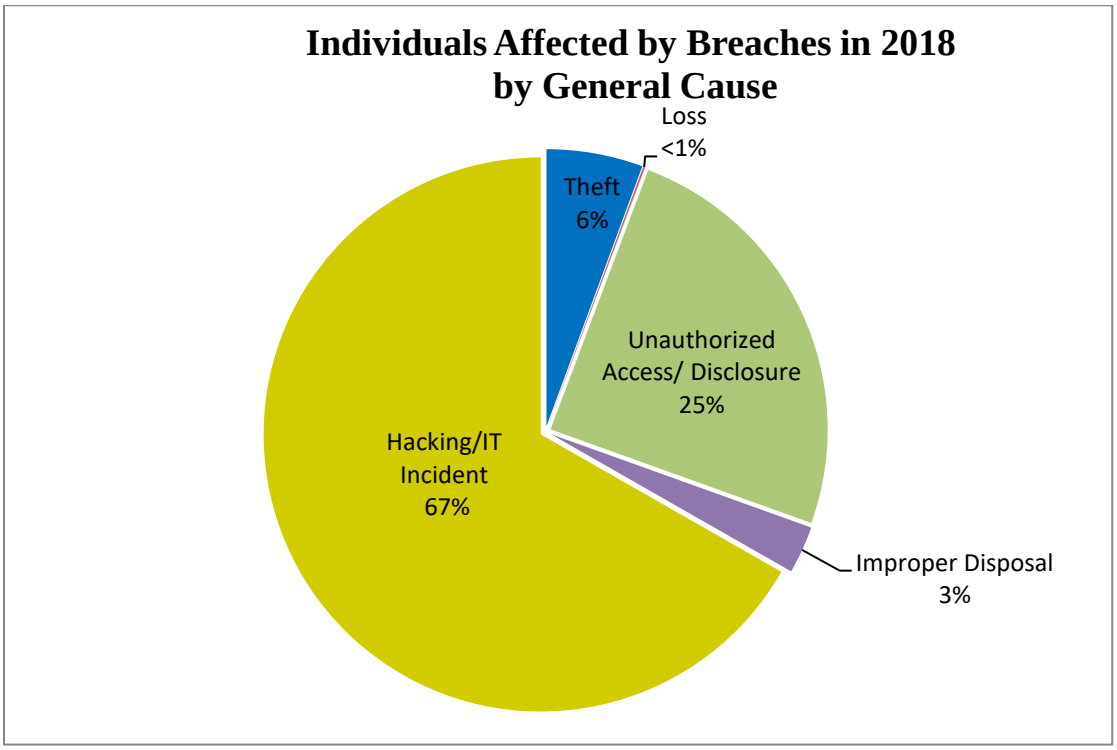

Figure 4

The 302 reports submitted to OCR for breaches occurring in 2018 described the following locations of the PHI (in order of frequency):

(1) E-mail (102 reports (34%) affecting 2,931,840 individuals (24%));
(2) Paper (69 reports (23%) affecting 1,156,602 individuals (9%));
(3) Network server (51 reports (17%), affecting 5,263,302 individuals (43%));
(4) Other (31 reports (10%) affecting 2,312,683 individuals (19%));[7]
(5) Laptop computer (17 reports (6%), affecting 73,848 individuals (< 1%));
(6) Desktop computer (11 reports (4%) affecting 309,298 individuals (3%));
(7) Electronic medical record (11 reports (4%), affecting 91,041 individuals (1%)); and
(8) Other portable electronic device (10 reports (3%), affecting 57,987 individuals (<1%)).

See Figures 5 and 6.

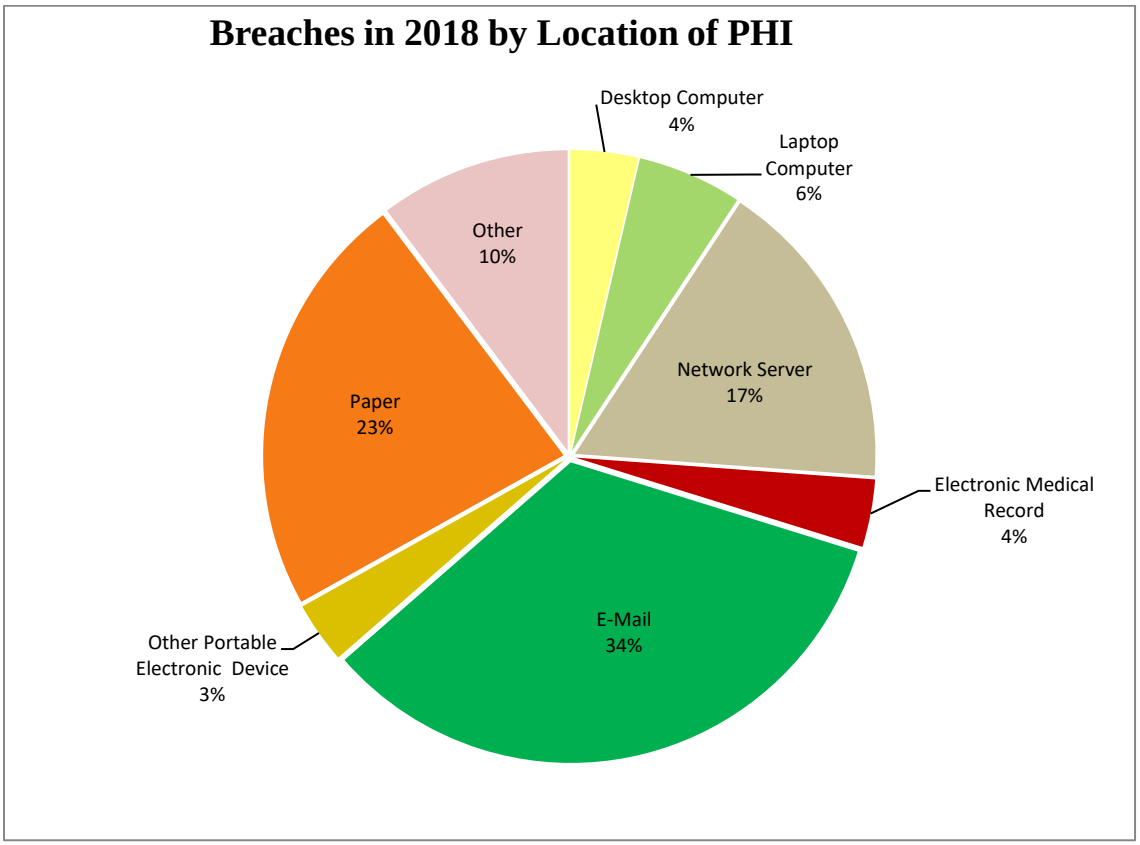

Figure 5

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

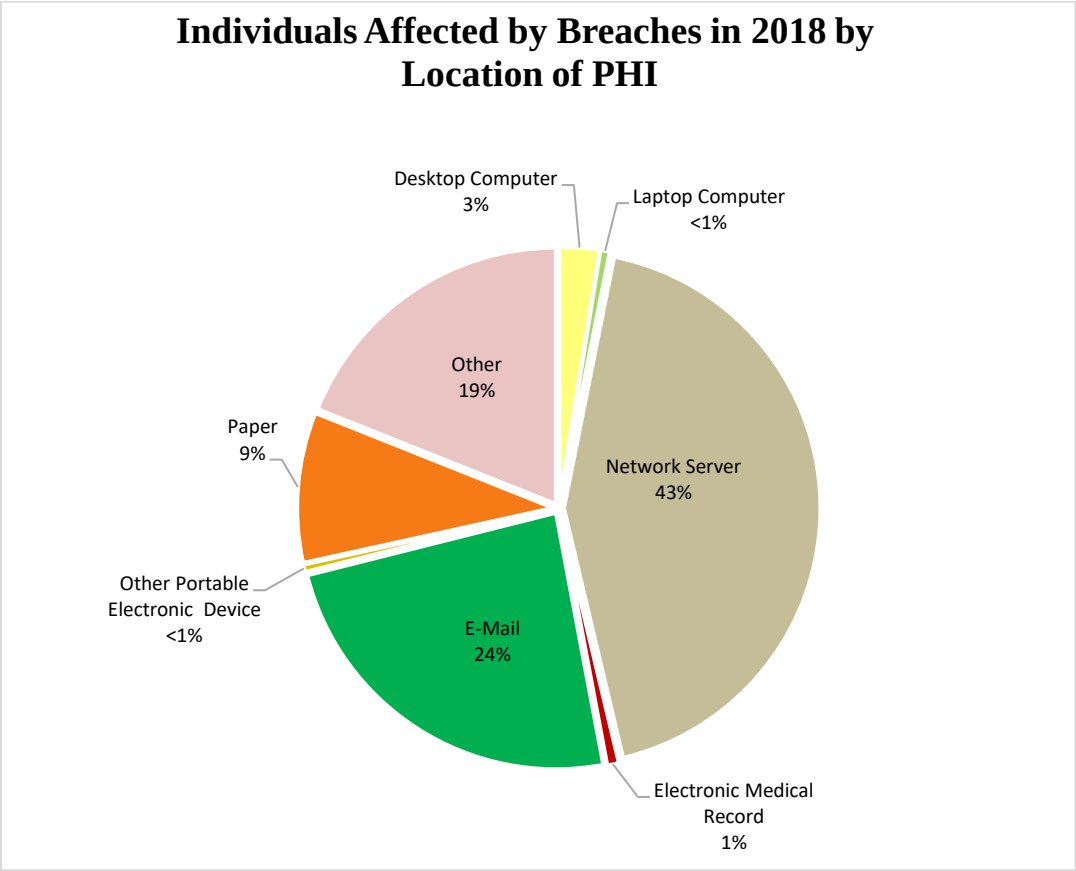

Figure 6

Largest breaches in 2018 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 scenarios reported for each cause.

Hacking/IT Incident of Electronic Equipment or Network Server: The largest breach in 2018 resulting from a hacking/IT incident involved a hacker who penetrated the server of a business associate. The breach incident affected approximately 2,652,537 individuals. Other hacking/IT incidents involved the use of malware, ransomware, phishing (e.g., employees opening email attachments that contained viruses), and the posting of PHI to public websites.

Theft: The largest breach in 2018 resulted from a break-in in which the offices of the covered entity were ransacked and items were stolen or vandalized. The intruder subsequently set the building on fire which resulted in permanent damage of paper and electronic medical records as well as other forms of PHI and ePHI. The theft affected approximately 582,174 individuals. The most reported cases of theft were of laptops and paper records. In the case of laptops, most incidents resulted from a lack of proper security measures. For paper records, most incidents involved the burglarizing of offices and storage facilities.

Improper Disposal: The largest reported improper disposal incident in 2018 resulted from the improper disposal of medical records affecting 301,000 individuals. An investigation by a covered entity revealed that abandoned medical records were left unsecured in various locations throughout the building and were discovered when the new owners were preparing the building for demolition. Other improper disposal breaches involved paper records containing PHI disposed in recycling or trash bins rather than authorized shred bins.

Unauthorized Access or Disclosure of PHI: The largest breach in 2018 involving the unauthorized access or disclosure of PHI affected approximately 1,248,263 individuals. In this case, a covered entity discovered that the 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, and misdirected communications.

Loss of PHI: The largest breach reported as a loss in 2018 resulted from the loss of a binder that contained the PHI of approximately 5,019 individuals. Other incidents in this category involved paper and electronic media that could not be located.

Remedial Action Reported

For breaches affecting 500 or more individuals that occurred in 2018, 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 to prevent future breaches:

- Revising policies and procedures;
- Improving physical security by installing new security systems or 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;
- 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 2018, notification to OCR was required no later than March 2, 2019.

Breaches involving fewer than 500 individuals for 2018

OCR received 63,098 reports of under 500 breaches during calendar year 2018. These smaller breaches affected 296,948 individuals. Of these breaches submitted to OCR occurring in 2018, by covered entity type, outline the following (in order of frequency):

(1) Health Care Providers (56,076 reports (89%) affecting 223,888 individuals (75%));
(2) Health Plans (4,410 reports (7%) affecting 40,468 individuals (14%));
(3) Business Associates (2,527 reports (4%) affecting 32,366 individuals (11%)); and
(4) Health Care Clearinghouses (85 reports (<1%) affecting 226 individuals (<1%)).

See Figure 7.

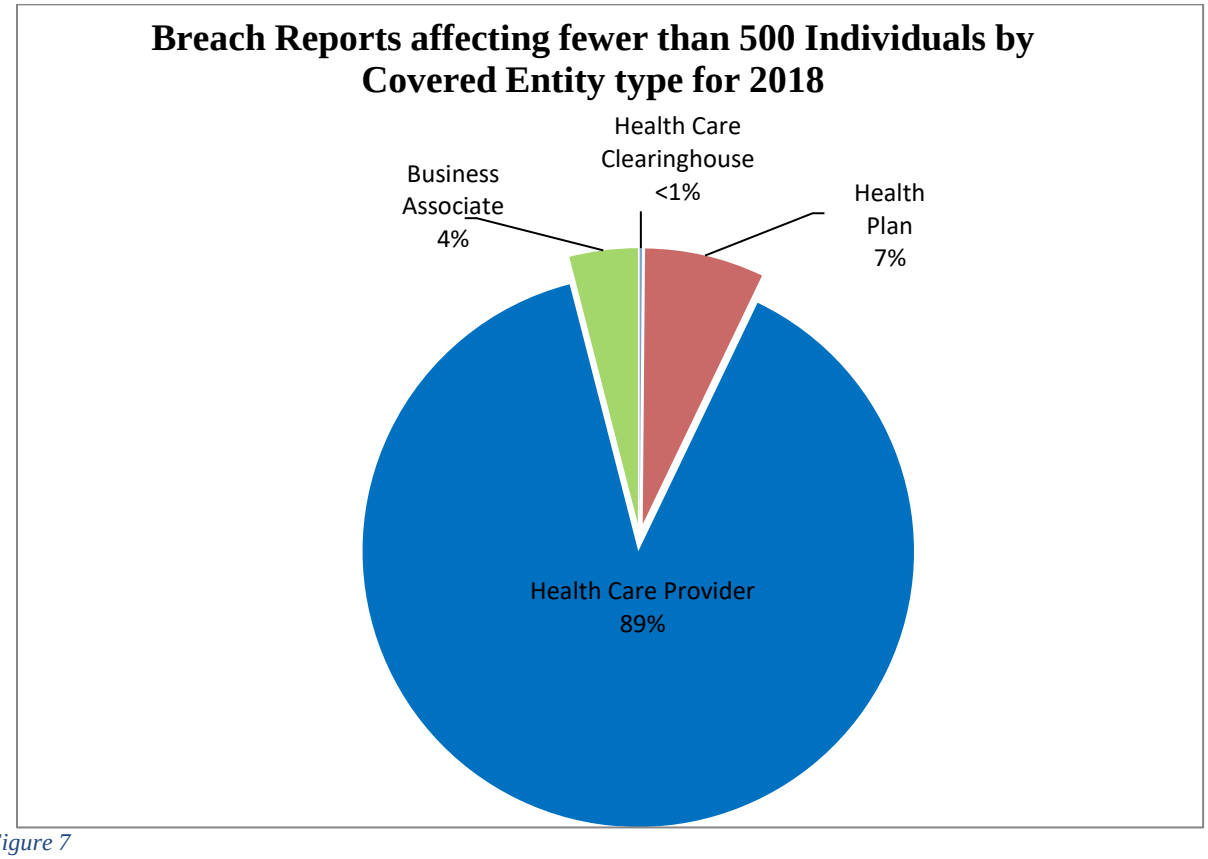

Figure 7

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

(1) Unauthorized access or disclosure (57,009 reports (90%) affecting 185,314 individuals (62%));
(2) Loss (3,100 reports (5%) affecting 21,213 individuals (7%));
(3) Hacking/IT incident (1,378 reports (2%) affecting 46,276 individuals (16%));
(4) Theft (1,098 reports (2%) affecting 35,804 individuals (12%)); and
(5) Improper disposal (513 reports (1%) affecting 8,341 individuals (3%)).

See Figures 8 and 9.

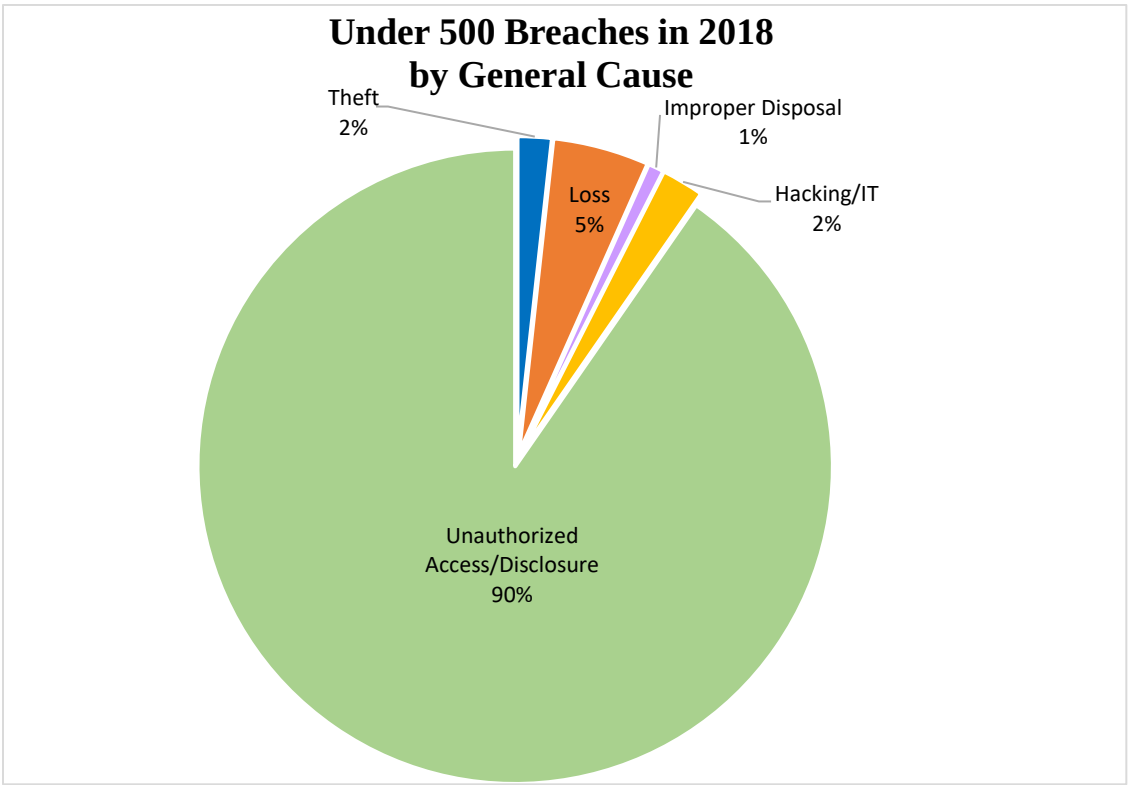

Figure 8

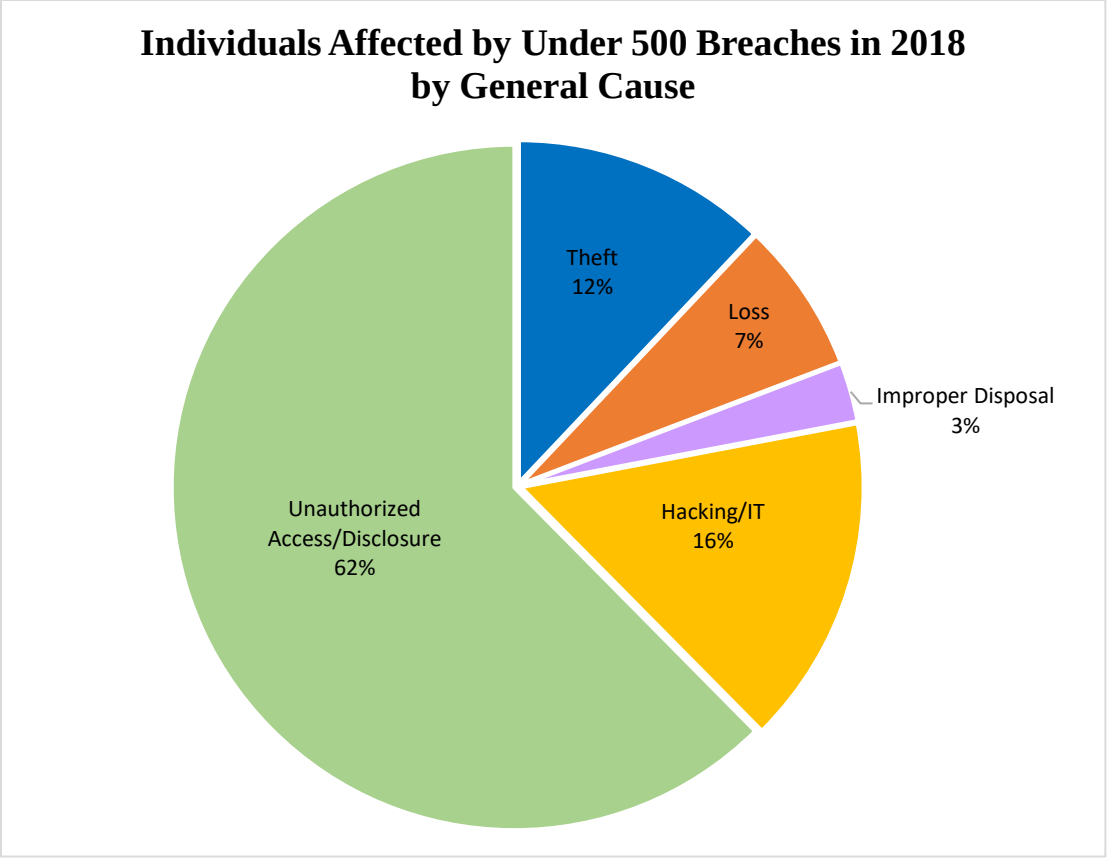

Figure 9

The 63,098 reported breaches affecting fewer than 500 individuals described the following locations of the PHI (in order of frequency):

(1) Paper (41,800 reports (66%) affecting 124,763 individuals (42%));
(2) Other (8,404 reports (13%) affecting 40,904 individuals (14%));[8]
(3) Electronic medical record (7,218 reports (11%) affecting 24,965 individuals (8%));
(4) E-mail (3,367 reports (5%) affecting 68,922 individuals (23%));
(5) Desktop computer (889 reports (1%) affecting 10,730 individuals (4%));
(6) Other portable electronic device (810 reports (1%) affecting 8,880 individuals (3%));
(7) Network server (409 reports (1%) affecting 9,065 individuals (3%)); and
(8) Laptops (201 reports (< 1%) affecting 8,719 individuals (3%)).

See Figures 10 and 11.

[8] See Note 7, above.

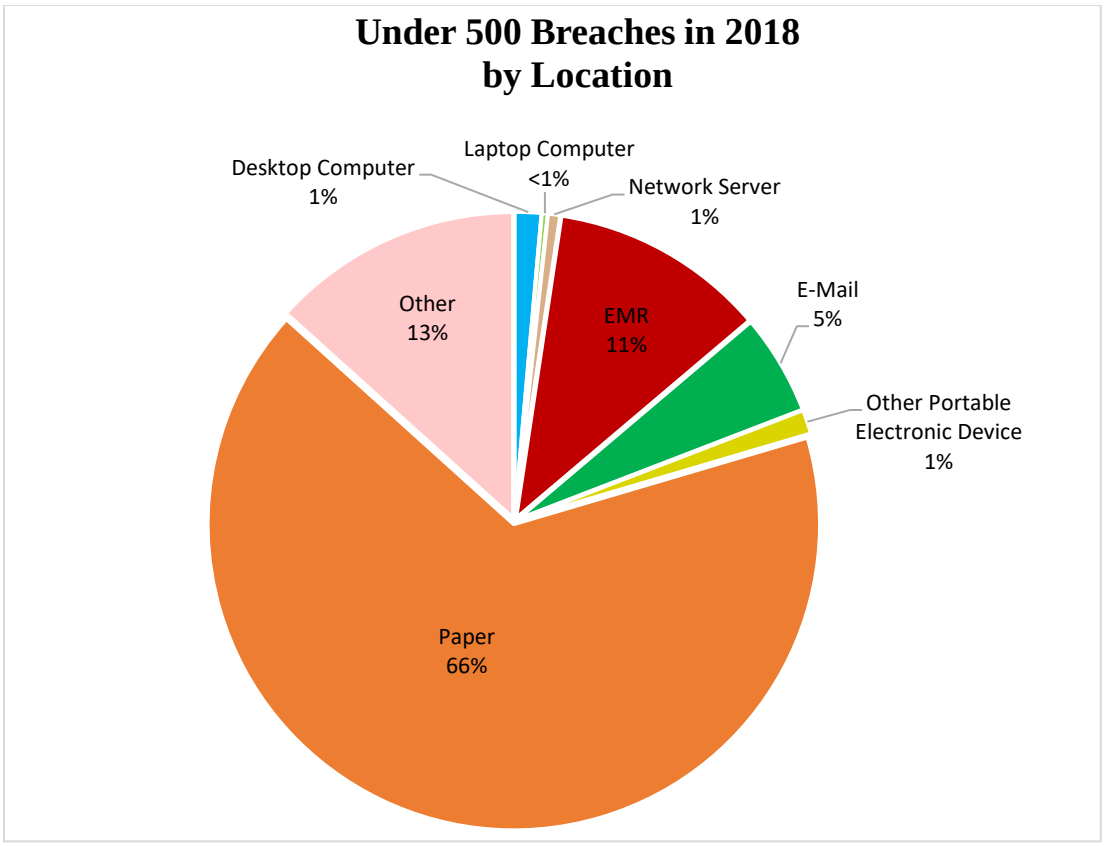
Under 500 Breaches in 2018
by Location
Desktop Computer
1%
Laptop Computer
<1%
Network Server
1%
E-Mail
5%
Other Portable
Electronic Device
1%
EMR
11%
Other
13%
Paper
66%

Figure 10

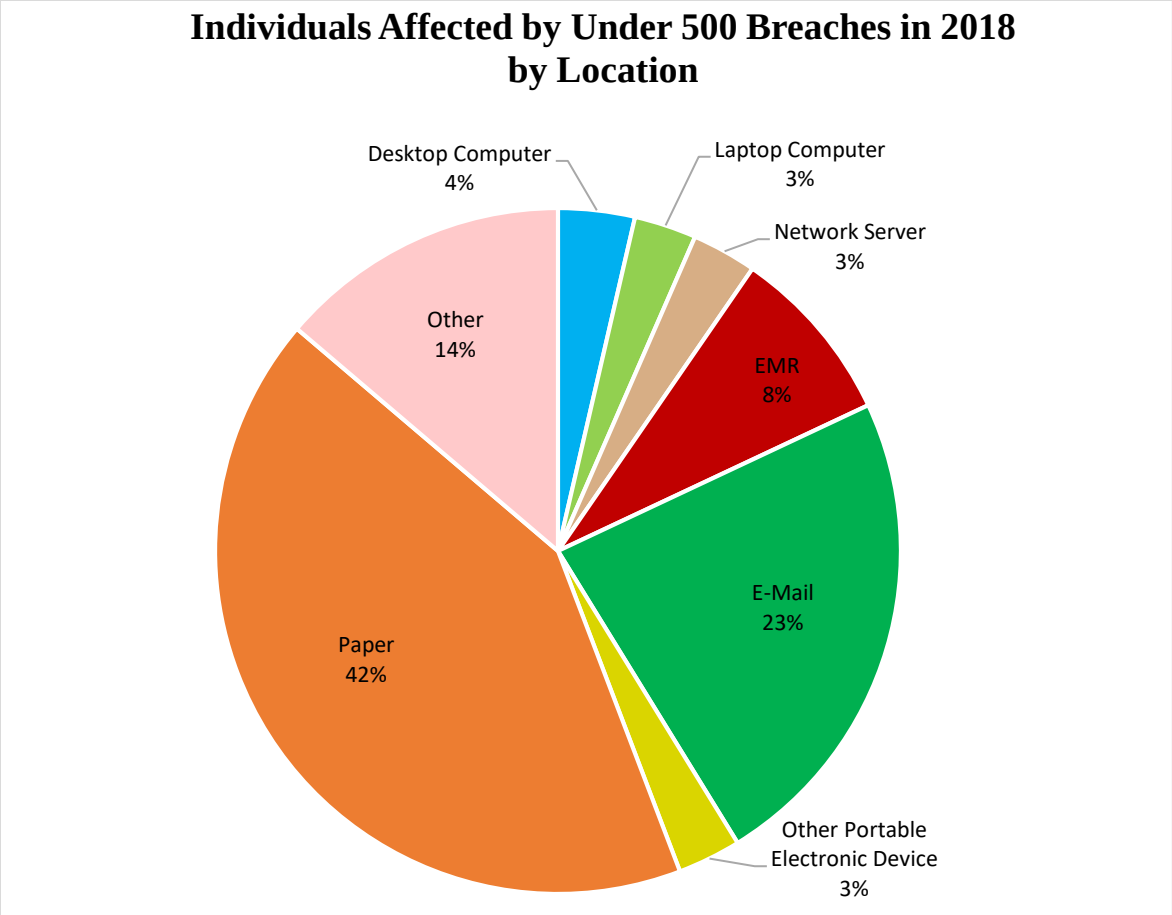

Figure 11

Details on Breaches involving fewer than 500 individuals for 2018

As in previous years, incidents reported for 2018 also 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. In addition to investigating all breaches affecting more than 500 or more individuals, OCR completed 26 breach investigations involving fewer than 500 individuals in 2018.

Cases Investigated and Action Taken

To fulfill its statutory obligation, OCR opened investigations into all of the 302 breaches affecting 500 or more individuals that occurred in 2018. OCR also opened 17 investigations into breaches affecting fewer than 500 individuals. OCR closed 431 investigations resulting from

breach reports after achieving voluntary compliance, through corrective action and technical assistance, through resolution agreements, or because no violation had occurred. Specific details about the cases that were resolved in 2018 with resolution agreements or civil money penalties can be found at the appendix at the end of this report. Additional information on OCR's compliance and enforcement works may be found in OCR's Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance for Calendar Year 2018.

Lessons Learned

The breach reports submitted to OCR offer insight into areas of vulnerability in protections for the privacy and security of individuals' health information. Covered entities and business associates should consider the following HIPAA Security Rule standards that were identified in OCR investigations in 2018 as areas needing improvement.

- Risk Analysis and Risk Management. Conducting an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of the electronic protected health information (ePHI) held by covered entities and business associates is a foundational requirement of the HIPAA Security Rule. However, OCR's investigations continue to identify the lack of a proper risk analysis as a major contributing factor in breaches to health data. In many instances, the technologies or locations involved in a breach of ePHI were not considered or were considered inadequately in the breached entity's risk analysis. Additionally, OCR's investigations often find that the entity took no or inadequate actions to mitigate the identified risks that led to a breach. Implementing security measures to reduce identified risks and vulnerabilities in accordance with the entity's risk management is also a requirement of the HIPAA Security Rule.

- Evaluation. The HIPAA Security Rule requires covered entities and business associates to conduct technical and non-technical evaluations in response to environmental or operational changes affecting the security of ePHI. OCR's investigations have found instances where entities have migrated ePHI to an unsecure server or application without conducting an evaluation to determine how the security of its ePHI would be affected. In some of these cases, OCR found that the ePHI was accessible without a password or other means of authentication, thus exposing the ePHI to unauthorized access, which resulted in a breach. It is imperative that entities understand how changes introduced into their operations or environment affect the security of ePHI and take appropriate steps to ensure such changes do not weaken the security of the entity's ePHI.

- Access Control. Implementing technical access controls to allow access to PHI only to those persons and entities that are permitted access to PHI is a requirement of the HIPAA Security Rule. However, OCR's investigations into breaches frequently find evidence of access controls that were not implemented. OCR's investigations have also noted that entities are not considering access controls at the network level. Network access controls, including segmentation, can impede malicious activities thereby potentially delaying and reducing the impact of an intruder or malicious software.

- Information System Activity Review. The number of breaches affecting 500 or more individuals as a result of hacking or IT incidents increased 282% from 2014 to 2018 (39 breach reports in 2014 vs. 149 breach reports in 2018). If an entity's network is breached and a malicious actor gains access to its internal systems, being alerted to, and reviewing, the actor's malicious activities is critical to being able to effectively halt, and recover from, an attack. Entities regulated by HIPAA are required to regularly review information system activity. However, OCR's investigations continue to reveal that entities are deficient in their implementation of these required review processes. Further, in addition to malicious outsiders, an effective information system activity review process can also identify the potential malicious activity of insiders (e.g., employees, contractors). The threat from malicious insiders remains a prevalent and growing concern in the healthcare sector.

- Security Incident Procedures. Entities regulated by HIPAA are required to identify and respond to suspected or known security incidents. Effective security incident plans prepare entities to effectively respond to a variety of incidents (e.g., malicious insiders, ransomware, advanced persistent threats). However, OCR's investigations note that entities fail to respond effectively and promptly to security incidents.

Summary and Conclusion

Hacking/IT incidents was the largest category of breaches occurring in 2018 involving 500 or more individuals, and also affected the most individuals. Additionally the data reveals that email is the largest category by location for breaches involving 500 or more individuals. For the under 500 breaches that occurred in 2018, unauthorized disclosures was the largest category of type of breach report, and paper records were the largest category by location.

The breach notification requirements are achieving their objectives of increasing public transparency and increasing accountability of covered entities and business associates. The reports submitted to OCR show 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. During 2018, in five cases resulting from breach reports, OCR entered into resolution

agreements/corrective action plans or imposed civil money penalties totaling more than $27.3 million.

APPENDIX

Resolution Agreements and Civil Money Penalties in 2018

Resolution Agreement with Fresenius Medical Care North America

Fresenius Medical Care North America (FMCNA) agreed to settle potential violations of the HIPAA Privacy and Security Rules with OCR. FMCNA paid $3.5 million and agreed to adopt a corrective action plan to correct deficiencies in its HIPAA compliance program. FMCNA is a provider of products and services for people with chronic kidney failure, with over 60,000 employees that serve over 170,000 patients. FMCNA's network is comprised of dialysis facilities, outpatient cardiac and vascular labs, and urgent care centers, as well as hospitalist and post-acute providers.

On January 21, 2013, FMCNA filed five separate breach reports for separate incidents occurring between February 23, 2012 and July 18, 2012 implicating the ePHI of five separate FMCNA-owned covered entities (FMCNA covered entities).

OCR's subsequent investigation found that FMCNA:

- Failed to conduct an accurate and thorough risk analysis of potential risks and vulnerabilities to the confidentiality, integrity, and availability of all of its ePHI;
- Impermissibly disclosed ePHI without an authorization;
- Failed to implement policies and procedures to address security incidents;
- Failed to implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI;
- Failed to implement a mechanism to encrypt and decrypt ePHI; and
- Failed to safeguard its facilities and equipment for unauthorized access, tampering, and theft.

In addition to a $3.5 million settlement, FMCNA agreed to:

- Complete a risk analysis and risk management plan to comply with the HIPAA Privacy and Security Rule;
- Revise policies and procedures to comply with the HIPAA Security Rule; and
- Train workforce members on the revised policies and procedures.

This settlement occurred in January 2018.

Civil Money Penalty (CMP) imposed on The University of Texas MD Anderson Cancer Center

A HHS Administrative Law Judge (ALJ) ruled that The University of Texas MD Anderson Cancer Center (MD Anderson) violated the HIPAA Privacy and Security Rules and granted judgment to OCR on all issues, and confirmed the imposition of a CMP on MD Anderson in the amount of $4,348,000. This is the second judgment in OCR's history of HIPAA enforcement.

MD Anderson is both a degree-granting academic institution and a comprehensive cancer treatment and research center located at the Texas Medical Center in Houston. OCR investigated MD Anderson following three separate data breach reports in 2012 and 2013 involving the theft of an unencrypted laptop from the residence of an MD Anderson employee and the loss of two unencrypted USB thumb drives containing the unencrypted ePHI of over 33,500 individuals. OCR's investigation found that MD Anderson had written encryption policies going back to 2006 and that MD Anderson's own risk analyses had found that the lack of device-level encryption posed a high risk to the security of ePHI. Despite the encryption policies and high risk findings, MD Anderson did not begin to adopt an enterprise-wide solution to implement encryption of ePHI until 2011, and even then it failed to encrypt its inventory of electronic devices containing ePHI between March 24, 2011 and January 25, 2013. The ALJ agreed with OCR's findings and the CMP.

The ALJ issued a decision upholding the CMP in June 2018. MD Anderson appealed the ALJ's decision, which was subsequently affirmed. MD Anderson filed an appeal with the U.S. Court of Appeals for the Fifth Circuit, which is currently pending.

Resolution Agreement with Anthem

Anthem, Inc. agreed to pay $16 million and take substantial corrective action to settle potential violations of the HIPAA Privacy and Security Rules after a series of cyberattacks led to the largest U.S. health data breach in history and exposed the ePHI of almost 79 million people.

The $16 million settlement is nearly three times the previous highest settlement of $5.55 million in 2016.

Anthem is an independent licensee of the Blue Cross and Blue Shield Association operating throughout the United States and is one of the nation's largest health benefits companies, providing medical care coverage to one in eight Americans through its affiliated health plans. This breach affected ePHI that Anthem, Inc. maintained for its affiliated health plans and many other covered entity health plans.

On March 13, 2015, Anthem filed a breach report with OCR detailing that it discovered cyber-attackers had gained access to its IT system via an undetected continuous and targeted cyberattack for the apparent purpose of extracting data. Anthem discovered cyber-attackers had infiltrated its system through spear phishing emails sent to an Anthem subsidiary after at least one employee responded to the malicious email and opened the door to further attacks. OCR's investigation revealed that the cyber-attackers stole the ePHI of almost 79 million individuals, including names, social security numbers, medical identification numbers, addresses, dates of birth, email addresses, and employment information.

Further, OCR's investigation revealed that Anthem:

- Failed to implement appropriate measures for detecting hackers to prevent, detect, contain, and correct security violations;
- Failed to implement strong password policies and procedures;
- Failed to monitor and respond to security incidents in a timely fashion;
- Failed to conduct an enterprise-wide risk analysis; and
- Failed to implement adequate minimum access controls to prevent access to sensitive ePHI.

In addition to the $16 million settlement, Anthem agreed to:

- Develop, maintain, and revise if necessary written policies and procedures to comply with the HIPAA Privacy Rule;
- Train workforce members on the revised policies and procedures; and
- Post a copy of the revised policies and procedures on its intranet.

This settlement occurred in October 2018.

Resolution Agreement with Advanced Care Hospitalists

Advanced Care Hospitalists PL (ACH) agreed to pay $500,000 and adopt a substantial corrective action plan to settle potential violations of the HIPAA Privacy and Security Rules. ACH provides contracted internal medicine physicians to hospitals and nursing homes in Florida. ACH provided services to more than 20,000 patients annually and employed between 39 and 46 individuals during the relevant timeframe.

Between November 2011 and June 2012, ACH engaged the services of an individual that presented himself as a representative of a Florida-based company named Doctor's First Choice Billings, Inc. (First Choice). The individual provided medical billing services to ACH using First Choice's name and website, but allegedly without any knowledge or permission of First Choice's owner.

On February 11, 2014, a local hospital notified ACH that patient information was viewable on the First Choice website, including name, date of birth and social security number. In response, ACH was able to identify at least 400 affected individuals and asked First Choice to remove the ePHI from its website. ACH filed a breach notification report with OCR on April 11, 2014, stating that 400 individuals were affected; however, after further investigation, ACH filed a supplemental breach report stating that an additional 8,855 patients could have been affected.

OCR's investigation revealed that ACH:

- Failed to enter into a business associate agreement with the medical billing service as required by HIPAA;
- Failed to adopt policies requiring business associate agreements until April 2014; and
- Failed to conduct a risk analysis or implement security measures.

In addition to the monetary settlement, ACH agreed to:

- Adopt and implement business associate agreements with all vendors;
- Complete an enterprise-wide risk analysis; and
- Develop comprehensive policies and procedures to comply with the HIPAA Rules.

This settlement occurred in September 2018.

Resolution Agreement with Cottage Health

Cottage Health agreed to pay $3 million and adopt a substantial correction action plan to settle potential violations of the HIPAA Security Rules. Cottage Health operates Santa Barbara Cottage Hospital, Santa Ynez Cottage Hospital, Goleta Valley Cottage Hospital, and Cottage Rehabilitation Hospital, in California. OCR received two notifications from Cottage Health regarding breaches of unsecured ePHI affecting over 62,500 individuals, one in December 2013 and another in December 2015.

The first breach arose when ePHI on a Cottage Health server was accessible from the Internet. OCR's investigation determined that security configuration settings of the Windows operating system permitted access to files containing ePHI without requiring a username and password. As a result, patient names, addresses, dates of birth, diagnoses, conditions, lab results and other treatment information were available to anyone with access to Cottage Health's server. The second breach occurred when a server was misconfigured following an IT response to a troubleshooting ticket, exposing unsecured ePHI over the Internet. This ePHI included patient names, addresses, dates of birth, social security numbers, diagnoses, conditions, and other treatment information.

OCR's investigation revealed that Cottage Health:

- Failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the ePHI;
- Failed to implement security measures sufficient to reduce risks and vulnerabilities to an appropriate level;
- Failed to perform periodic technical and non-technical evaluations in response to environmental or operational changes affecting the security of ePHI; and
- Failed to obtain a written business associate agreement with a contractor that maintained ePHI on its behalf.

In addition to the monetary settlement, Cottage Health agreed to:

- Conduct an enterprise-wide risk analysis;
- Develop a risk management plan;
- Implement processes for the evaluation of environmental and operational changes;
- Implement and distribute policies and procedures for protecting PHI; and
- Train all workforce members who have access to PHI.

This settlement occurred in December 2018.