Annual Report to Congress on Breaches of Unsecured Protected Health Information

For Calendar Year 2020

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

Executive Summary

Overview
This report summarizes key HIPAA enforcement activities undertaken by the HHS Office for Civil Rights during the 2020 calendar year. The Annual Report to Congress on Breaches of Unsecured Protected Health Information identifies the number and nature of breaches of unsecured protected health information (PHI) that were reported to the Secretary of HHS during the year and the actions taken in response to those breaches.

Summary
OCR received 656 notifications of breaches affecting 500 or more individuals, representing an increase of 61% from the number of reports received in calendar year 2019. These reported breaches affected a total of approximately 37,641,403 individuals. The most commonly reported category of breaches was hacking, and the largest breach of this type involved approximately 3,500,000 individuals. OCR also received 66,509 reports of breaches affecting fewer than 500 individuals, with unauthorized access or disclosure reported as the most frequent type of breach reported. These smaller breaches affected a total of 312,723 individuals.

OCR initiated investigations into all 656 breaches affecting 500 or more individuals, as well as 22 breaches involving fewer than 500 individuals. OCR completed 547 investigations, achieving voluntary compliance through corrective action and technical assistance, resolution agreements, or after determining no violation occurred. OCR resolved eight breach investigations with Resolution Agreements/Corrective Action Plans or the imposition of civil money penalties, which resulted in more than $13 million in collections.

Recommendations
There is continued need for regulated entities to improve compliance with the HIPAA Security Rule standards and implementation specifications of risk analysis and risk management, information system activity review, audit controls, security awareness and training, and authentication. All of these compliance concerns were identified as areas needing improvement in 2020 OCR breach investigations.

As it was the previous two years, hacking/IT incidents remain the largest category of breaches occurring in 2020 affecting 500 or more individuals, and also affected the most individuals, comprising 68% of the reported breaches. Network servers is the largest category by location for breaches involving 500 or more individuals. For the under 500 breaches, unauthorized access or disclosures was the largest category of type of breach report, and paper records was the largest by location.

Background

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 2020.

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 mandates that the Secretary issue guidance specifying the technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized persons. The guidance issued by the Secretary identifies encryption and destruction processes as tested by the National Institute of Standards and Technology as the two technologies and methodologies for rendering PHI unusable, unreadable, or indecipherable to unauthorized persons.[1] 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).

The Office for Civil Rights (OCR) is the office within the Department that is responsible for administering and enforcing the HIPAA Privacy, Security, and Breach Notification Rules.

[1] https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/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, 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.[3]

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.[4] 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] *See* 45 CFR § 164.402 (definition of "breach").

[4] 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

- **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 website 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.[5]

- **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.[6]

- **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

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.

[5] *See* 45 CFR § 164.404.

[6] *See* 45 CFR § 164.406.

are notified of the breach.[7] If a breach involves fewer than 500 individuals, covered entities 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.[8] 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's report to the covered entity 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.[9]

Summary of Breach Reports

This report describes the types and numbers of breaches reported to OCR that occurred between January 1, 2020, and December 31, 2020, and describes actions that have been taken by covered entities and business associates in response to these breaches.

This report generally describes 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 2020. 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, for 2020, in addition to requiring covered entities and business associates to take corrective action in hundreds of cases, OCR resolved eight breach investigations with resolution agreements/corrective action plans totaling more than $13 million in collections.

---

[7] *See* 45 CFR § 164.408(b).
[8] *See* 45 CFR § 164.408(c).
[9] *See* Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the HITECH Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 FR 5566, 5656 (January 25, 2013). *See also* 45 CFR § 164.410.

As shown in the table below, the number of breaches reported to OCR continues to increase. Between 2016 and 2020, the number of breaches affecting fewer than 500 individuals increased 14.52% and the number of breaches affecting 500 or more individuals rose 96.41%.

Year	Under 500 Breaches Reported	500+ Breaches Reported	Percentage Change in Under 500 Breaches Reported	Percentage Change in 500+ Breaches Reported
2020	66,509	656	6% increase	61% increase
2019	62,771	408	-.5% decrease	35% increase
2018	63,098	302	4.6% increase	-21.5% decrease
2017	60,332	385	4% increase	15% increase
2016	58,074	334	-	-
2016-2020 Increase (Percentage change)	14.52%	96.41%	-	-

Source: Current and previous Reports to Congress

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 656 reports of such breaches for calendar year 2020,[10] which affected a total of approximately 37,641,403 individuals.[11]

[10] 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 2018 into 2020 would be reported with the 2020 figures).

[11] 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.

Breaches in 2020 Affecting 500 or More Individuals[12]

For the 656 breaches affecting 500 or more individuals in 2020, OCR received:

(1) 504 reports (77%) of breaches from health care providers (affecting 20,287,314 individuals (54%));
(2) 78 reports (12%) of breaches from business associates (affecting 10,938,223 individuals (29%));
(3) 72 reports (11%) of breaches from health plans (affecting 6,369,634 individuals (17%)); and
(4) 2 reports (<1%) of breaches from health care clearinghouses (affecting 46,232 individuals (<1%)).

See Figures 1 and 2.

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

HHS Office for Civil Rights
Breach Reports of Unsecured PHI Affecting 500 or more Individuals in 2020 by Percentage of Reports Received by Entity Type

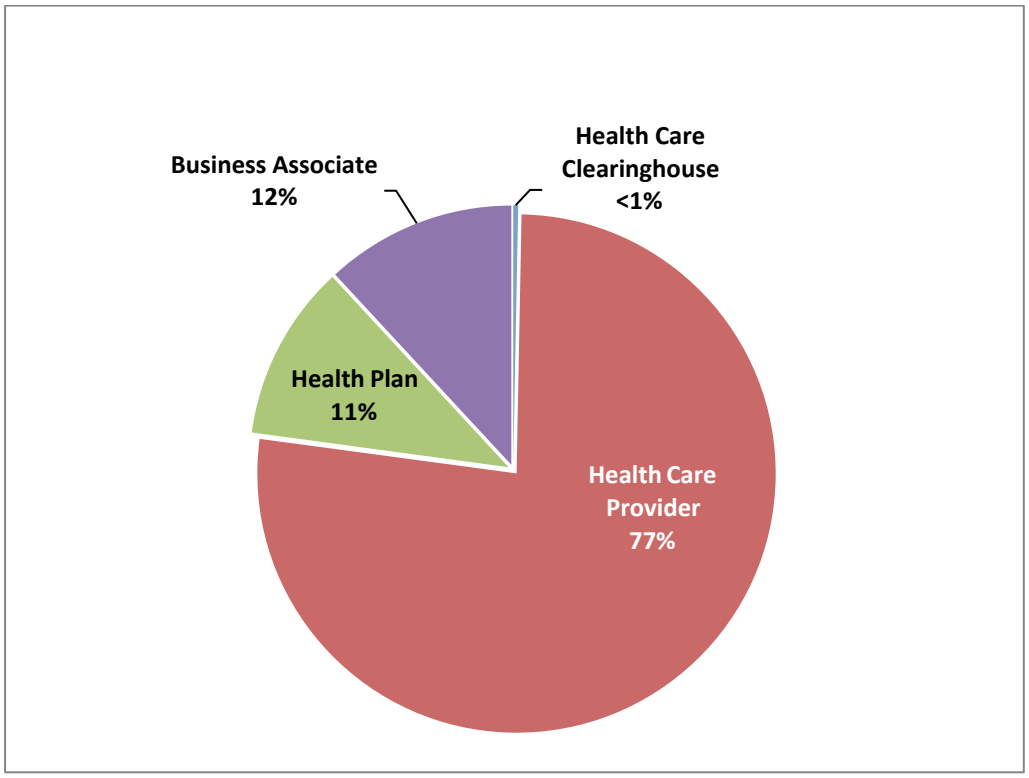

Figure 1

HHS Office for Civil Rights
Breach Reports of Unsecured PHI Affecting 500 or more Individuals in 2020 by Percentage of Individuals Affected by Entity Type

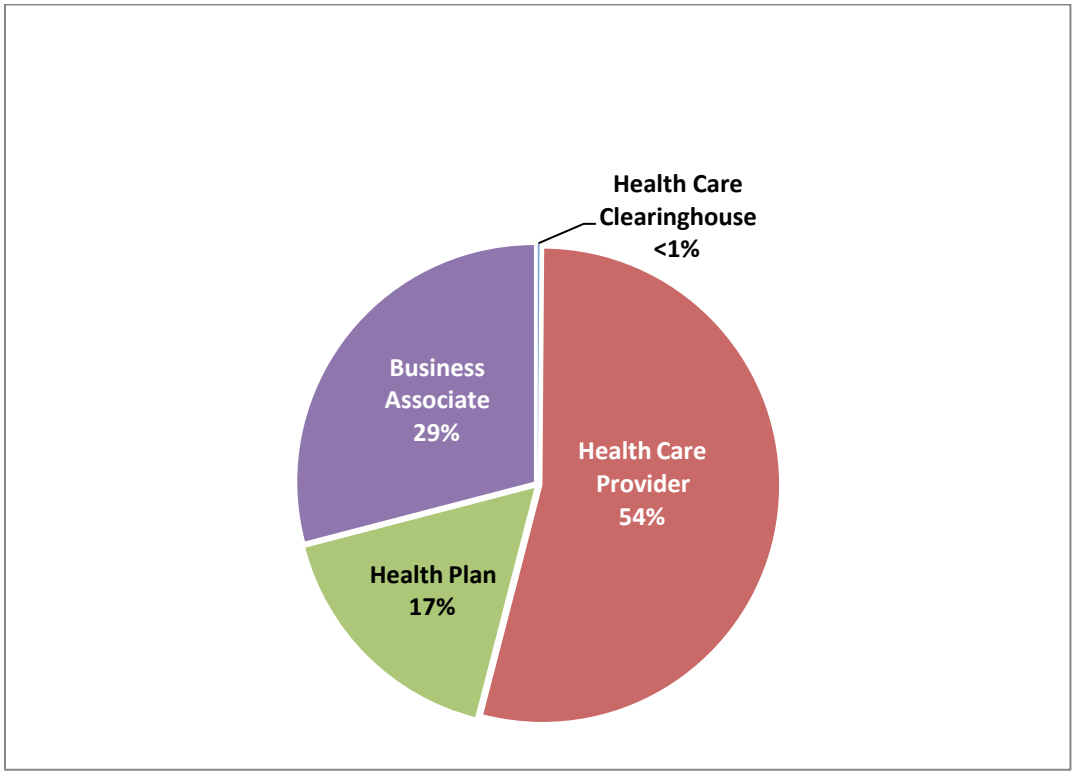

Figure 2

The 656 reports submitted to OCR for breaches affecting 500 or more individuals occurring in 2020 can be categorized by five general types or causes as follows (in order of frequency):[13]

(1) Hacking/IT incident of electronic equipment or a network server (444 reports (68%) affecting 34,265,326 individuals (91%));
(2) Unauthorized access or disclosure of records containing PHI (148 reports (23%) affecting 2,474,480 individuals (7%));
(3) Theft of electronic equipment/portable devices or paper containing PHI (36 reports (5%) affecting 155,161 individuals (<1%));
(4) Loss of electronic media or paper records containing PHI (16 reports (2%) affecting 176,169 individuals (<1%)); and
(5) Improper disposal of PHI (12 reports (2%) affecting 570,267 individuals (2%)).

See Figures 3 and 4.

HHS Office for Civil Rights
Breach Reports of Unsecured PHI Affecting 500 or more Individuals in 2020 by Percentage and Type of Breach

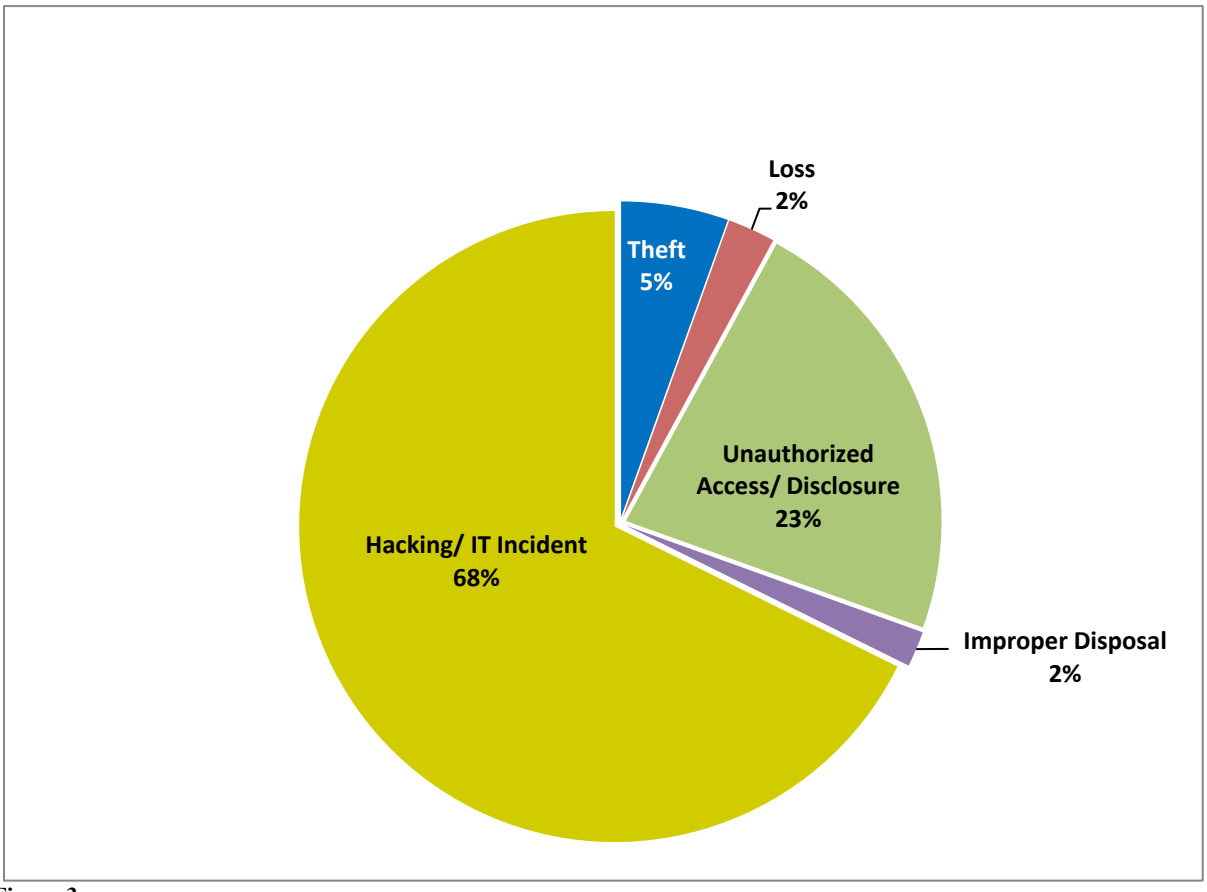

Figure 3

[13] Only one cause or type of breach can be selected in the breach report to HHS. Entities select the type of breach, using the definitions on the form in the HHS Breach Web Portal.

HHS Office for Civil Rights
Breach Reports of Unsecured PHI Affecting 500 or more Individuals in 2020 by Percentage of Individuals Affected and Type of Breach

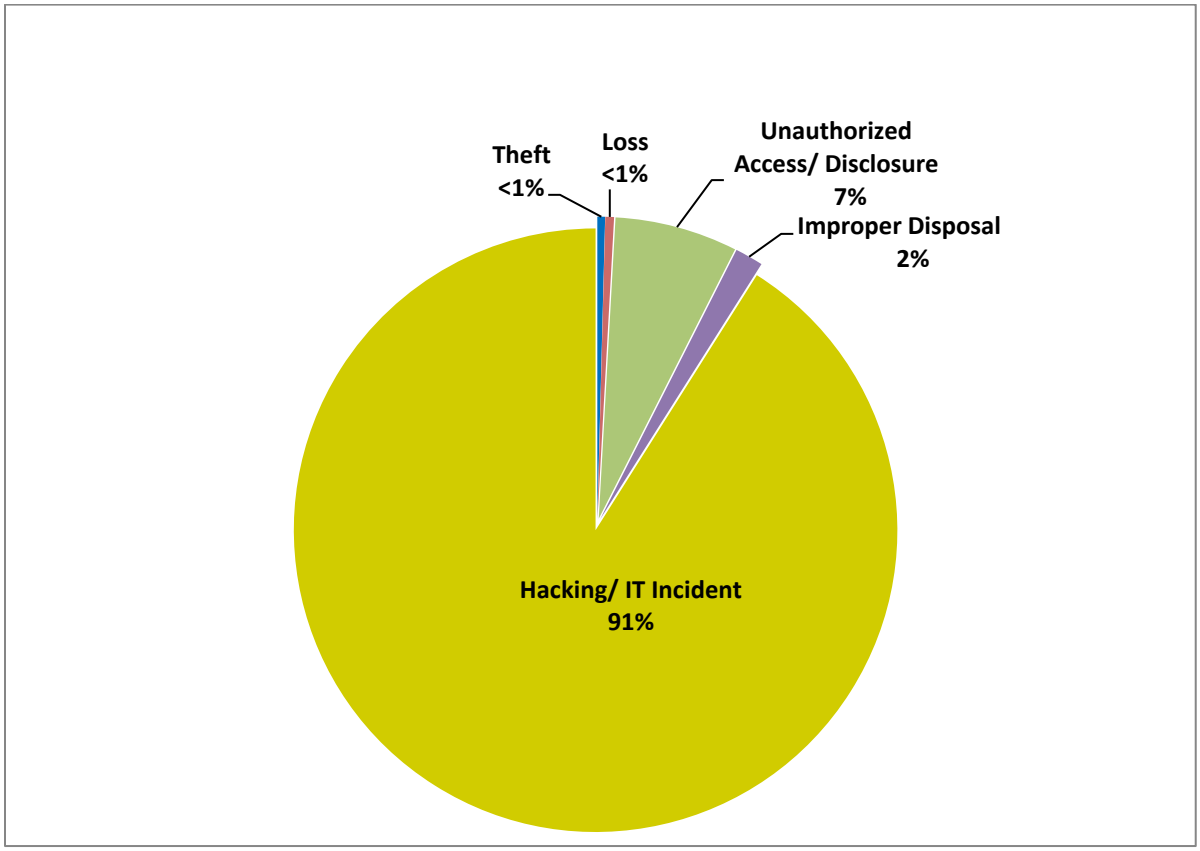

Figure 4

The 656 reports submitted to OCR for breaches occurring in 2020 described the following locations of the PHI (in order of frequency):[14]

(1) Network server (266 reports (41%), affecting 24,604,946 individuals (65%));
(2) E-mail (208 reports (32%) affecting 10,643,488 individuals (28%));
(3) Paper (78 reports (12%) affecting 855,131 individuals (2%));
(4) Electronic medical record (34 reports (5%) affecting 361,307 individuals (1%));[15]
(5) Other (28 reports (4%) affecting 443,267 individuals (1%));
(6) Desktop computer (20 reports (3%), affecting 574,723 individuals (2%));
(7) Laptop computer (11 reports (2%), affecting 51,762 individuals (< 1%)); and

[14] A breach may occur in more than one location. The reporting entity selects the main location of the breach in compiling this data.
[15] 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 disclosed.

(8) Other portable electronic device (11 reports (2%), affecting 106,779 individuals (<1%)).

See Figures 5 and 6.

HHS Office for Civil Rights
Breach Reports of Unsecured PHI Affecting 500 or more Individuals in 2020 by Percentage and Location of PHI

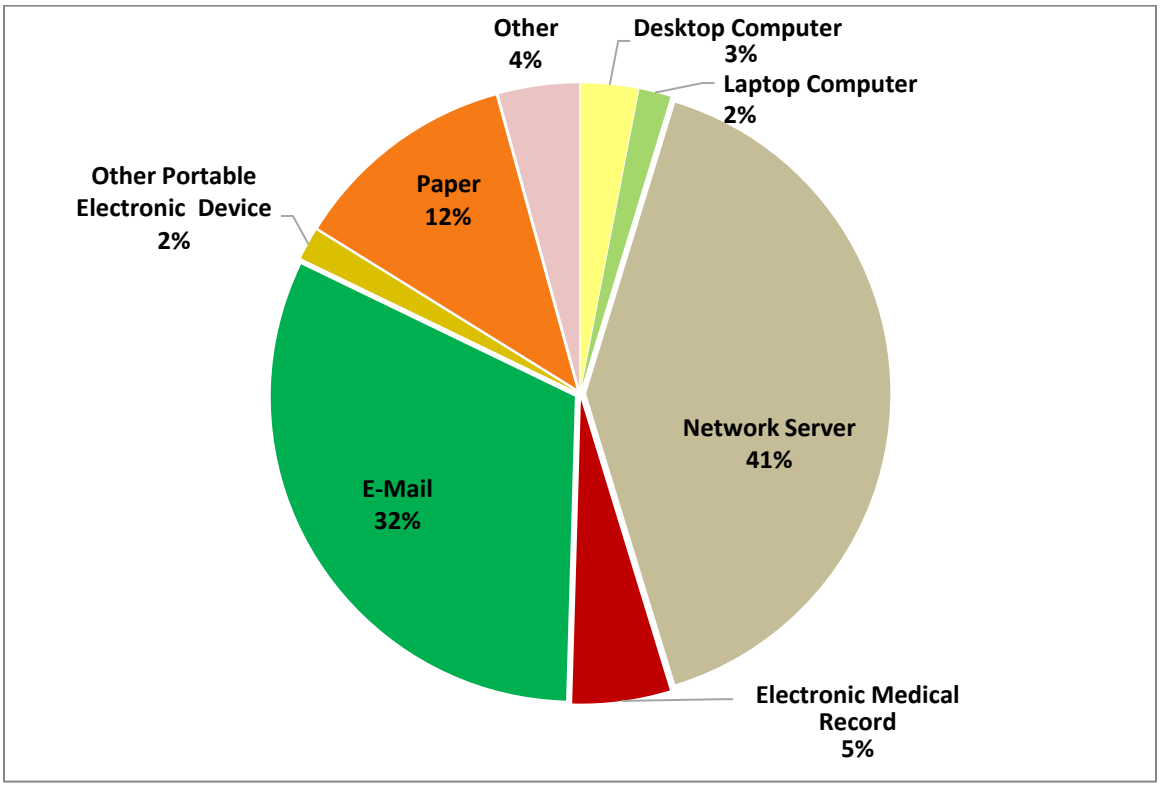

Figure 5

HHS Office for Civil Rights
Breaches of Unsecured PHI affecting Fewer Than 500 Individuals in 2020
by Individuals Affected by Location of PHI

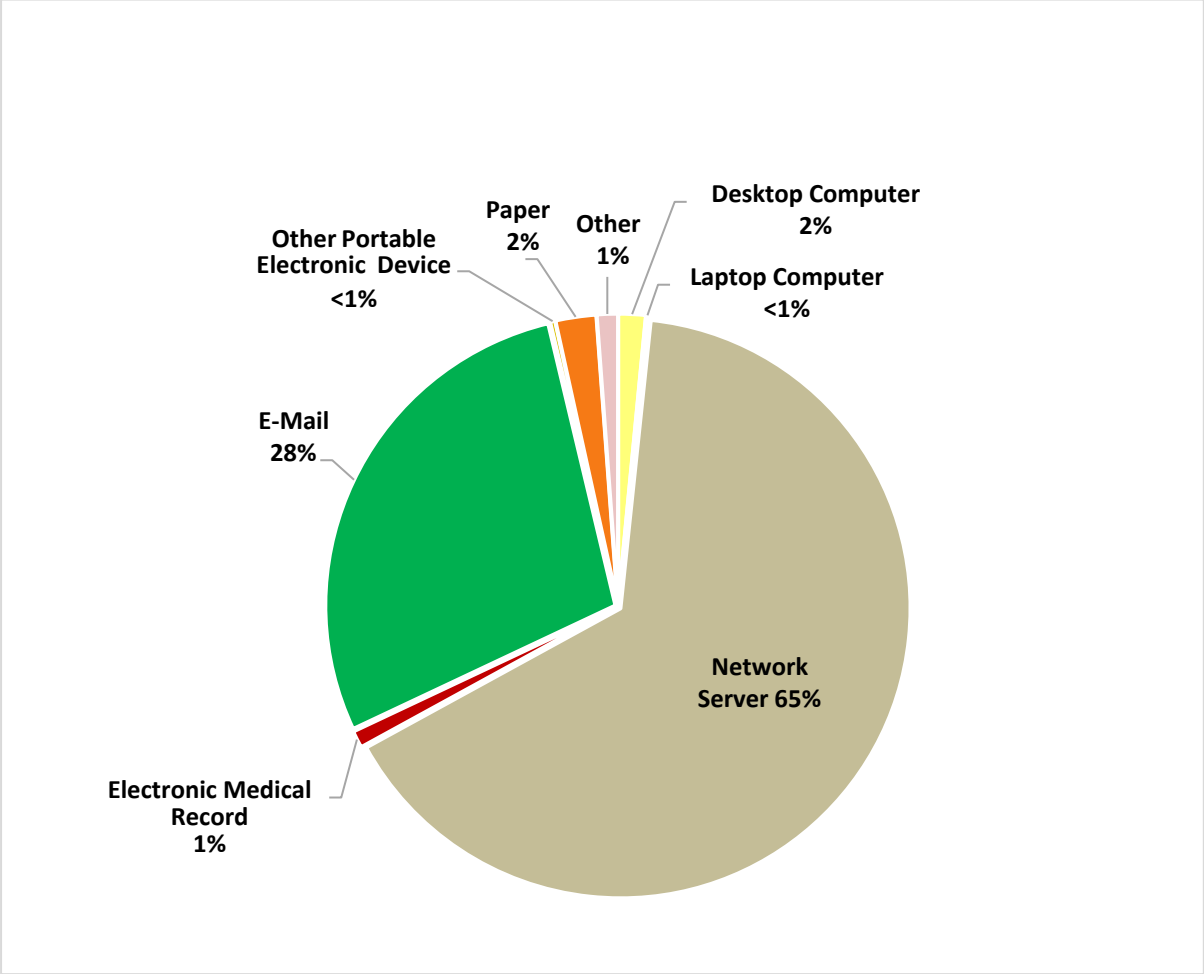

Figure 6

Largest breaches in 2020 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 2020 resulting from a hacking/IT incident involved a hacker who penetrated the server of a business associate containing PHI. The breach incident affected approximately 3,500,000 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.

Unauthorized Access or Disclosure of PHI: The largest breach in 2020 involving the unauthorized access or disclosure of ePHI affected approximately 1,474,000 individuals. An unauthorized individual accessed ePHI maintained in a business associate's email system. Other incidents of unauthorized access or disclosure involved employees impermissibly accessing records outside the scope of their job responsibilities, and misdirected communications.

Improper Disposal: The largest reported improper disposal incident in 2020 resulted from a business associate who improperly disposed of medical records by storing them in an unsecured barn. This breach affected 550,000 individuals. Other improper disposal breaches involved disposing of paper records containing PHI in trash bins rather than authorized shred bins.

Theft: The largest theft-related breach in 2020 resulted from the theft of cash registers (with hard drives that contain ePHI) and paper records containing PHI when multiple pharmacy locations were burglarized. The thefts affected approximately 80,176 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, such as a lack of access controls. For paper records, most incidents involved the burglarizing of offices and storage facilities.

Loss of PHI: The largest breach reported as a loss in 2020 resulted from the loss of medical records and vaccine consent forms that contained the PHI of approximately 26,234 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 2020, 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:

- Implementing multi-factor authentication for remote access;
- Revising policies and procedures;
- Training or retraining workforce members who handle PHI;
- Providing free credit monitoring and identity theft protection services 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 2020, notification to OCR was required no later than March 1, 2021.

Breaches involving fewer than 500 individuals for 2020

OCR received 66,509 reports of breaches affecting fewer than 500 individuals occurring in calendar year 2020. These smaller breaches affected 312,723 individuals. Set forth below are the breaches submitted to OCR by covered entity type (in order of frequency):

(1) Health Care Providers (59,936 reports (90%) affecting 249,850 individuals (80%));
(2) Health Plans (4,962 reports (7%) affecting 35,945 individuals (11%));
(3) Business Associates (1,542 reports (2%) affecting 26,646 individuals (9%)); and
(4) Health Care Clearinghouses (69 reports (<1%) affecting 282 individuals (<1%)).

See Figures 7 and 8.

HHS Office for Civil Rights
Breach Reports of Unsecured PHI affecting Fewer Than 500 Individuals in 2020 by Percentage and Covered Entity Type

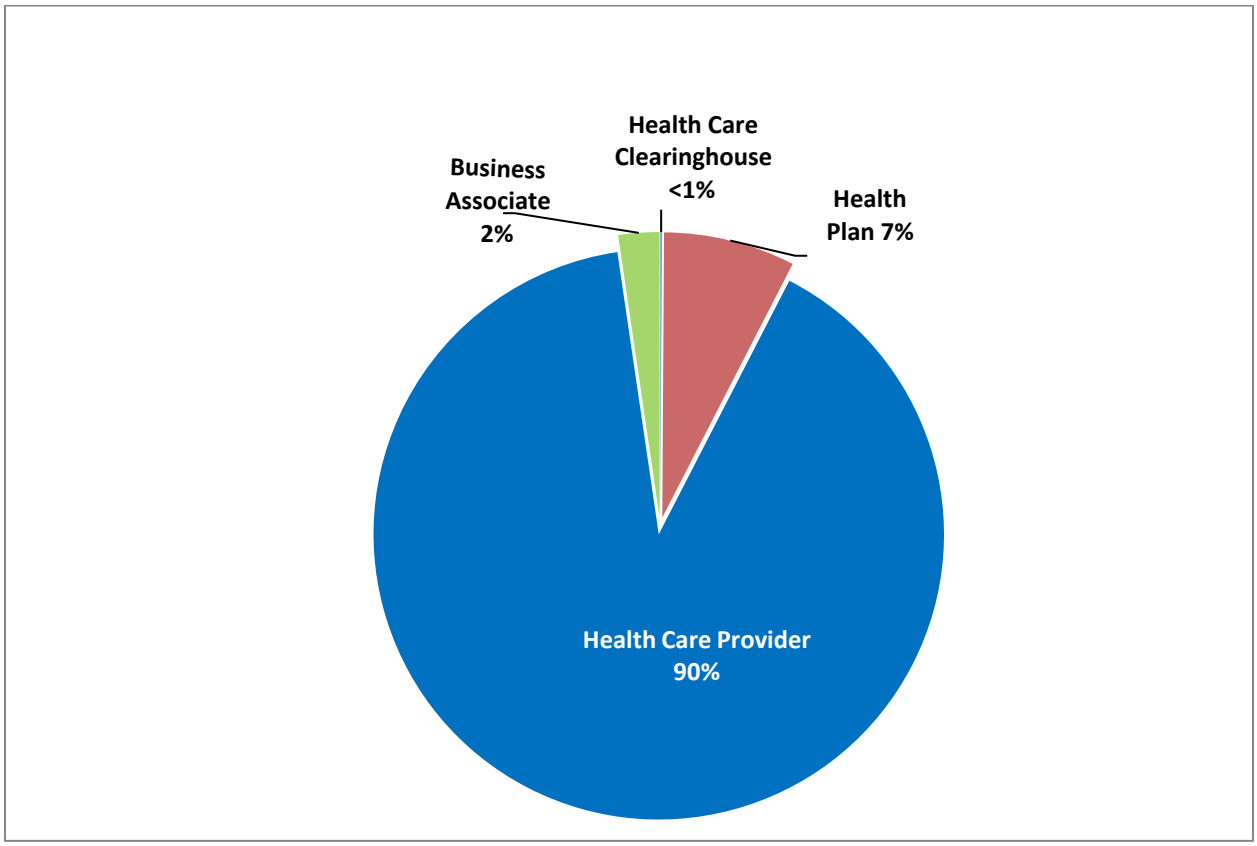

Figure 7

HHS Office for Civil Rights
Breach Reports of Unsecured PHI affecting Fewer Than 500 Individuals in 2020 by Percentage of Individuals Affected by Covered Entity Type

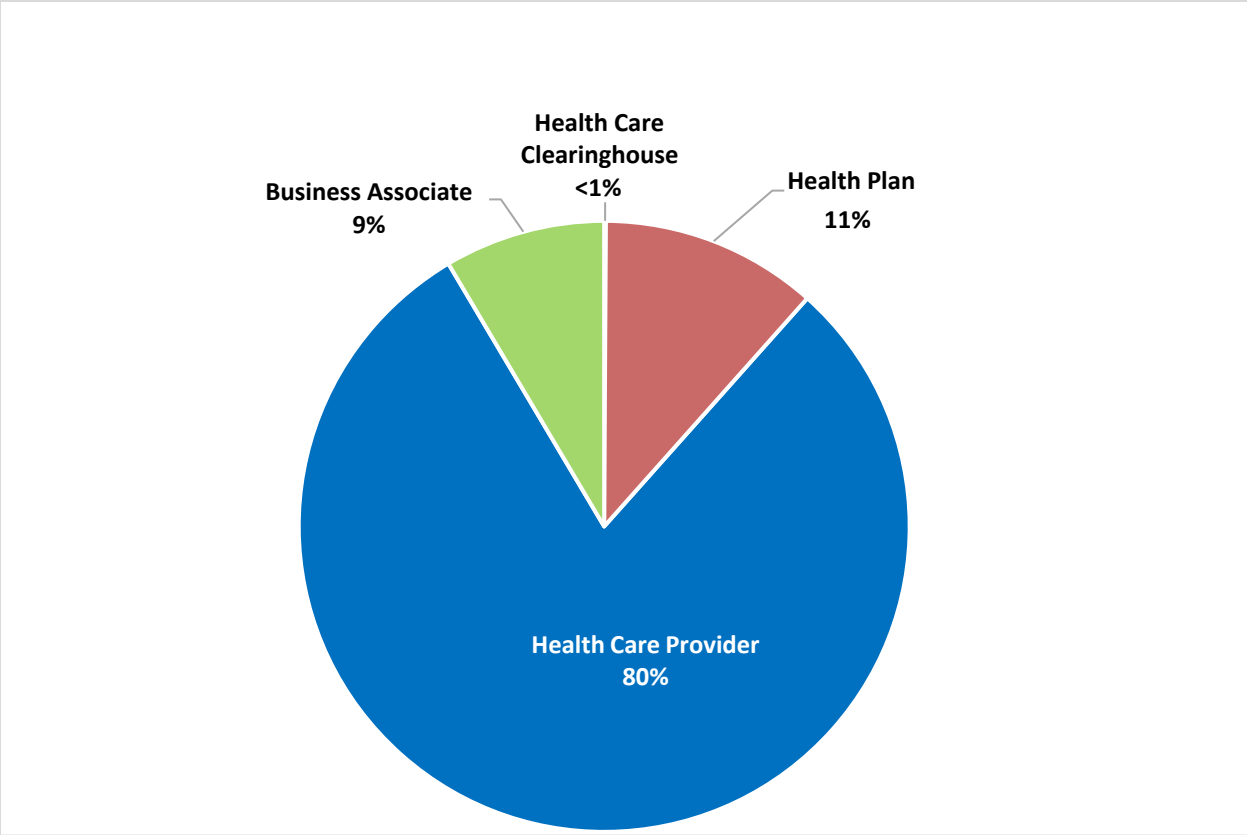

Figure 8

The most common causes or types of breach incidents (in order of frequency) for breaches affecting fewer than 500 individuals were:[16]

(1) Unauthorized access or disclosure (61,973 reports (93%) affecting 195,582 individuals (63%));
(2) Loss (2,662 reports (4%) affecting 16,541 individuals (5%));
(3) Theft (1,038 reports (2%) affecting 31,327 individuals (10%));
(4) Hacking/IT incident (665 reports (1%) affecting 62,633 individuals (20%)); and
(5) Improper disposal (171 reports (<1%) affecting 6,640 individuals (2%)).

See Figures 9 and 10.

[16] Only one cause or type of breach can be selected in the breach report to HHS. Entities select the type of breach, using the definitions on the form in the HHS Breach Web Portal.

HHS Office for Civil Rights
Breach Reports of Unsecured PHI affecting Fewer Than 500 Individuals in 2020 by Percentage and Type of Breach

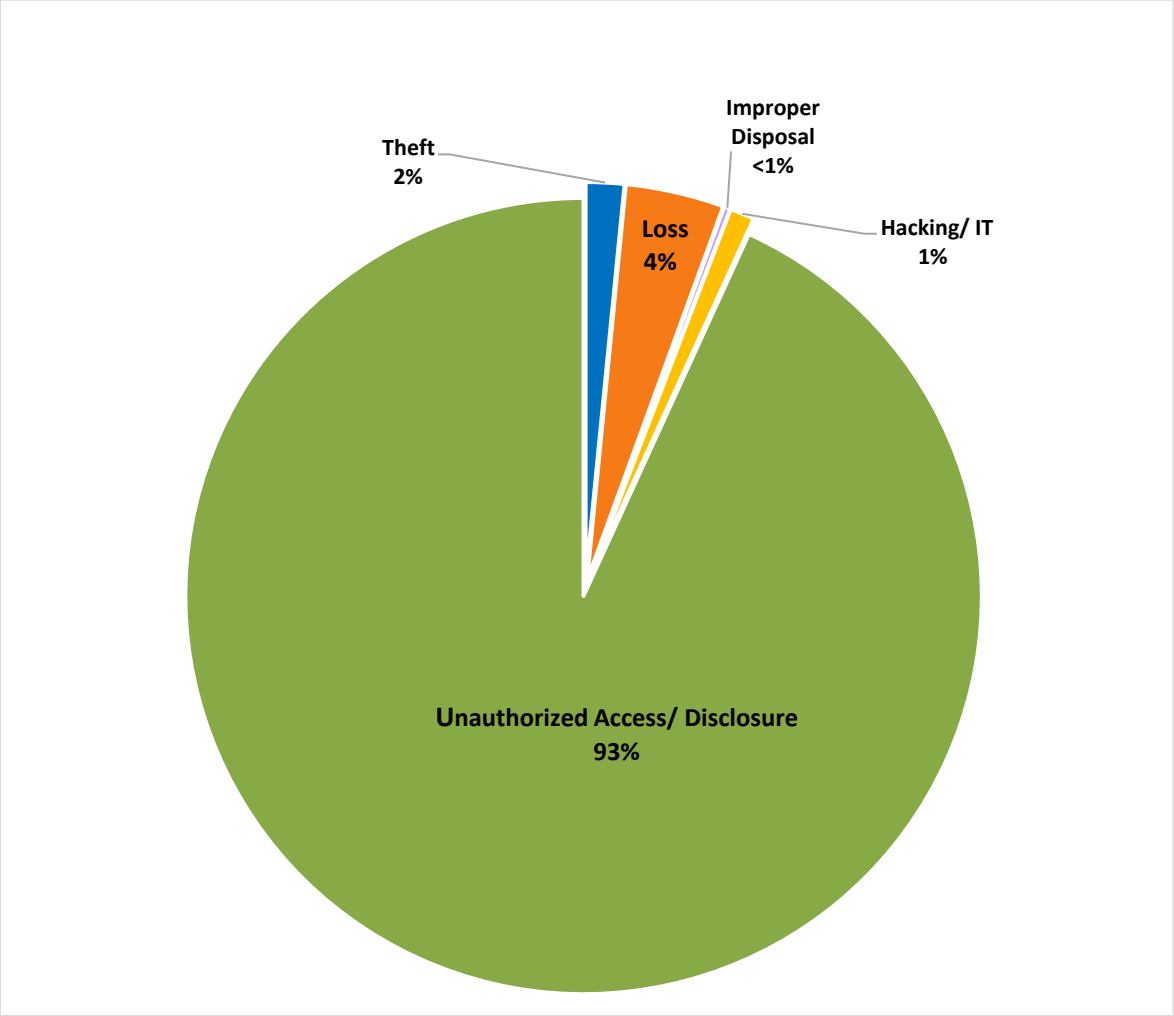

Figure 9

HHS Office for Civil Rights
Breach Reports of Unsecured PHI affecting Fewer Than 500 Individuals in 2020 by Percentage and Type of Breach

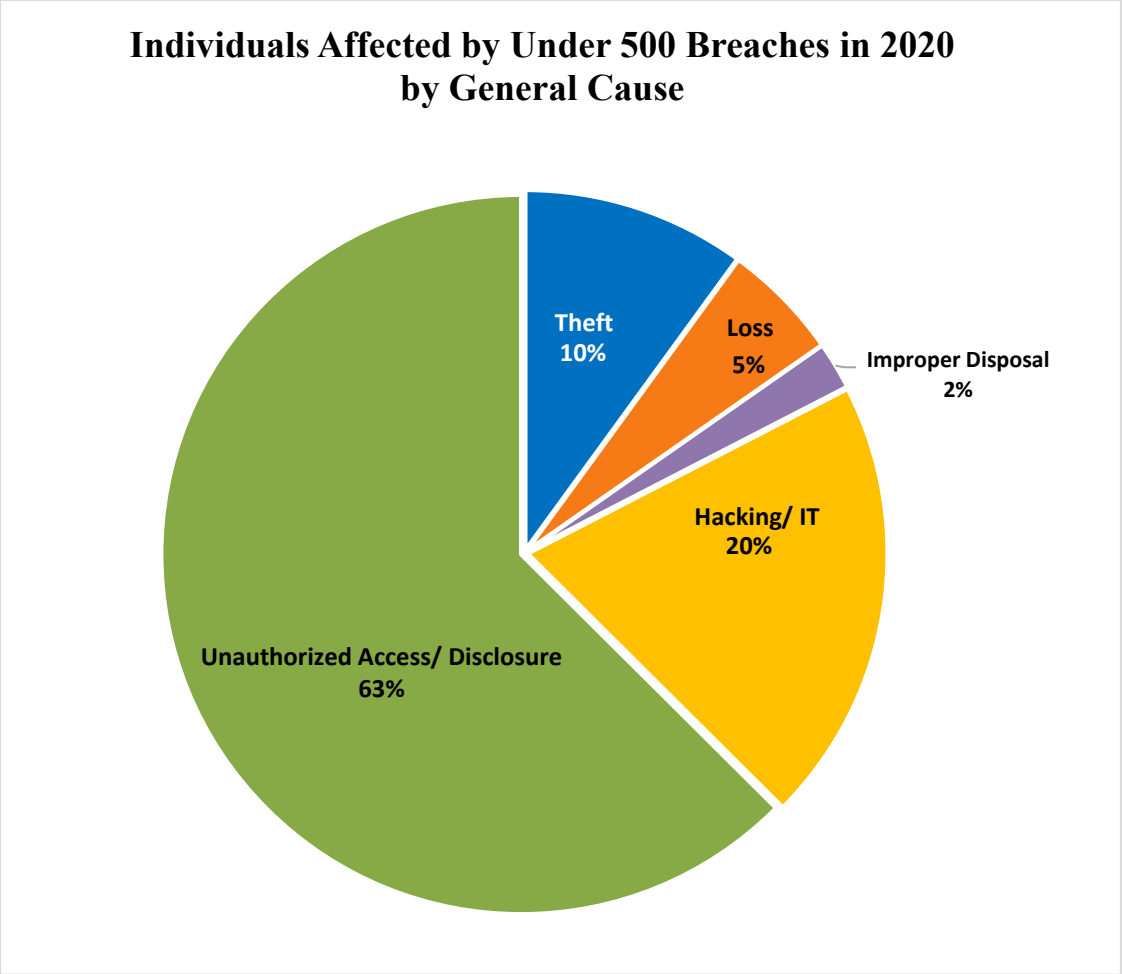

Figure 10

The 66,509 reported breaches affecting fewer than 500 individuals described the following locations of the PHI (in order of frequency):[17]

(1) Paper (44,292 reports (67%) affecting 114,968 individuals (37%));
(2) Electronic medical record (EMR) (8,017 reports (12%) affecting 28,758 individuals (9%));
(3) Other (7,788 reports (12%) affecting 35,704 individuals (11%));[18]
(4) E-mail (4,000 reports (6%) affecting 78,029 individuals (25%));

[17] A breach may occur in more than one location. The reporting entity selects the main location of the breach in compiling this data.
[18] See footnote 16 on description of "other" category.

(5) Desktop computer (872 reports (1%) affecting 13,004 individuals (4%));
(6) Other portable electronic device (769 reports (1%) affecting 4,744 individuals (2%));
(7) Network server (574 reports (1%) affecting 29,640 individuals (9%)); and
(8) Laptop computer (197 reports (< 1%) affecting 7,876 individuals (3%)).

See Figures 11 and 12.

HHS Office for Civil Rights
Breach Reports of Unsecured PHI affecting Fewer Than 500 Individuals in 2020 by Percentage and Type of Breach

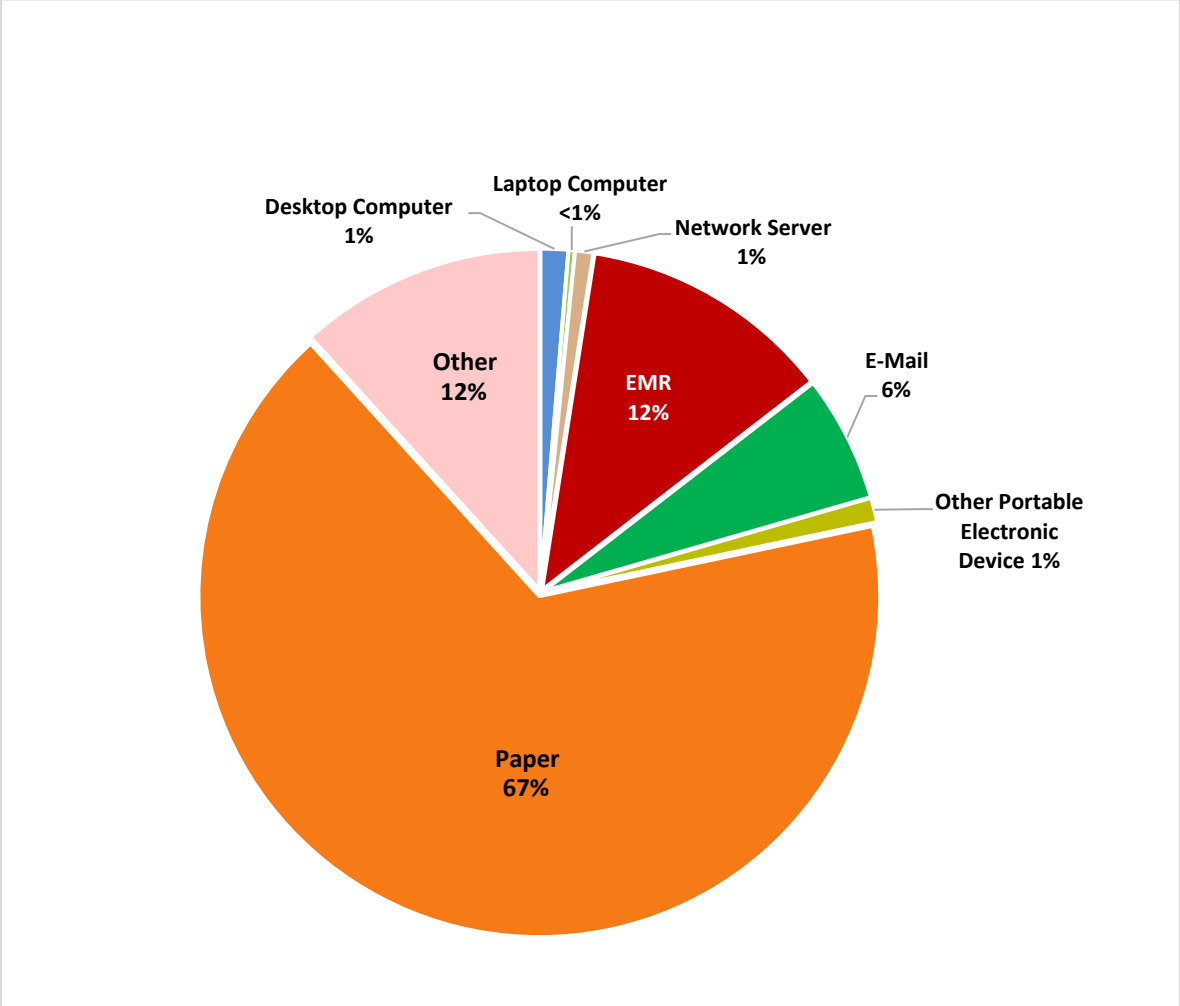

Figure 11

HHS Office for Civil Rights
Breaches of Unsecured PHI affecting Fewer Than 500 Individuals in 2020 by Individuals Affected by Location of PHI

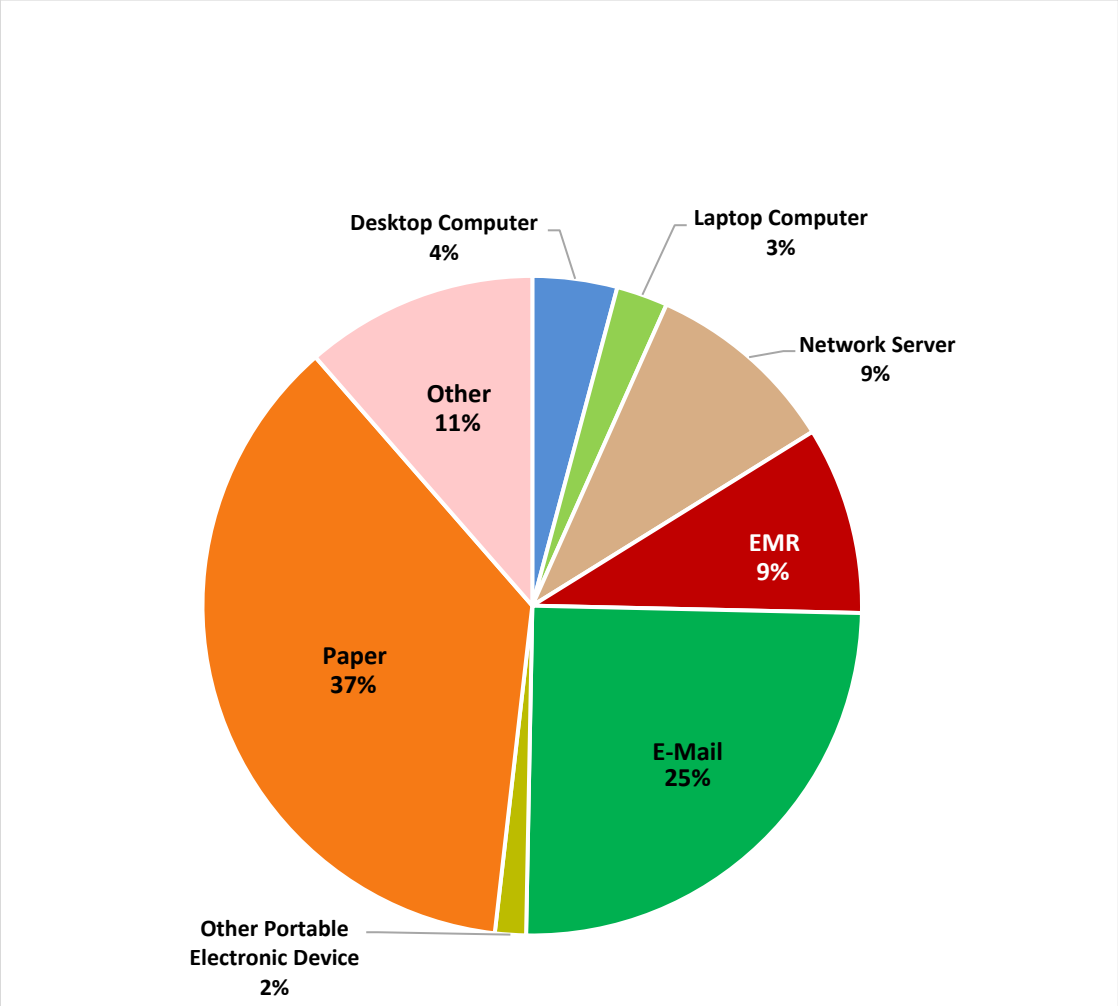

Figure 12

Details on breaches involving fewer than 500 individuals for 2020

As in previous years, incidents reported for 2020 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 addition, a large number of breach reports for 2020 were due to employees who impermissibly accessed the medical records of co-workers, family, friends, and other individuals without a business need. 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, training or retraining employees who handle PHI, and sanctioning employees.

In addition to investigating all breaches affecting 500 or more individuals, OCR completed 22 breach investigations involving fewer than 500 individuals in 2020.

Cases Investigated and Action Taken

OCR opened investigations into all of the 656 reported breaches affecting 500 or more individuals that occurred in 2020. OCR also opened 22 investigations into breaches affecting fewer than 500 individuals. OCR completed 547 investigations resulting from breach reports after achieving voluntary compliance, through corrective action and technical assistance, resolution agreements, or because no violation had occurred. Specific details about the cases that were resolved in 2020 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 work may be found in OCR's Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance for Calendar Year 2020.

Lessons Learned

The breach reports submitted to OCR offer insight into areas of vulnerability in protections for the privacy and security of individuals' protected health information. Covered entities and business associates should consider the following HIPAA Security Rule standards and implementation specifications that were identified in OCR investigations in 2020 as areas needing improvement.

- Risk Analysis and Risk Management. Deficient or non-existent risk analyses remained an area of concern and contributing factor to breaches of PHI throughout 2020. OCR's investigations uncovered numerous instances of entities that had never conducted a risk analysis or had conducted risk analyses that were not accurate and thorough as required by the HIPAA Security Rule. An inadequate risk analysis often leads to inadequate implementations of security measures to protect PHI. OCR's investigations discovered that entities lacking an accurate and thorough risk analysis frequently also had deficient risk management processes. The HIPAA Security Rule requires entities to implement security measures to reduce risks to its ePHI to a reasonable and appropriate level. But, even risks assessed as part of a deficient risk analysis would often go unmitigated as a result of an entity's inadequate risk management.

- Information System Activity Review. Breaches of PHI due to hacking continue to be the leading cause of breaches affecting 500 or more individuals reported to OCR. Early detection of cyber-attacks is critical to preventing successful hacking attempts and limiting the damage caused by a successfully infiltration into an entity's information technology systems. The HIPAA Security Rule requires covered entities and business associates to regularly review information system activity (e.g., access reports, audit logs, security incident tracking reports). When properly implemented, information system

reports and logs can document a hacker's intrusion and activities. The information system activity review process can not only help identify potential malicious attacks but can also aid in identifying suspicious activities of potential malicious insiders (e.g., workforce members, contractors). However, OCR continues to find that many entities are deficient in regularly reviewing information system activity.

- Audit Controls. An entity's information system activity review process relies on its information systems capturing and maintaining information system activity. The HIPAA Security Rule requires covered entities and business associates to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI. Yet, OCR's investigations discovered numerous instances of non-existent or deficient implementations of audit controls. Examples of OCR's findings included entities that only implemented audit logs on a narrow subset of information systems and audit log misconfigurations that led to gaps in logging a hacker's activities. Deficient audit control implementations reduce the visibility of information system activity such that an entity may not know what a hacker did and what systems the hacker accessed, thus impeding an entity response and recovery from a cyber-attack.

- Security Awareness and Training. Providing security awareness and training for all workforce members is a requirement of the HIPAA Security Rule. Security awareness and training is crucial to ensure workforce members (including management) are aware of security risks to PHI. Such training is even more important with the substantial increase of cyber-attacks, including ransomware, on health care entities. Social engineering attacks, including spoofing email to introduce malware into an environment (i.e., phishing), have been increasingly successful. Security training programs should educate workforce members and management on how to recognize and report cybersecurity threats such as phishing.

- Authentication. Verifying that a person or entity seeking access to ePHI is who they claim is required by the HIPAA Security Rule authentication standard. However, OCR's investigations have uncovered multiple instances of deficient authentication processes - some contributing to breaches of PHI. Examples of inadequate authentication include entities relying on weak password rules that allow easily discoverable passwords and poor implementation of web-based authentication schemes that allow access to ePHI without authentication. The increase in successful attacks that compromise remote access solutions demonstrates the need for strong, risk-based authentication implementations - especially for remote access solutions.

Summary and Conclusion

As it was the previous two years, hacking/IT incidents remain the largest category of breaches occurring in 2020 involving 500 or more individuals, and also affected the most individuals, comprising 68% of the reported breaches. Network servers is the largest category by location for breaches involving 500 or more individuals. For the under 500 breaches that occurred in 2020,

unauthorized access or disclosures was the largest category of type of breach report, and paper records was the largest 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.

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 2020, OCR resolved eight breach investigations with resolution agreements/corrective action plans or imposed civil money penalties totaling more than $13 million.[19]

[19] The eight cases were Steven A. Porter, MD, Metro Community Health Services dba Agape Health Services, Lifespan, Athens Orthopedic Clinic, CHSPSC, Premera Blue Cross, Aetna Life Insurance Company, and City of New Haven.

APPENDIX

Resolution Agreements[20] in 2020

Resolution Agreement with Steven A. Porter, M.D.

Steven A. Porter, M.D. (Porter), agreed to pay $100,000 and take corrective action to settle potential violations of the HIPAA Security Rule. Dr. Porter's medical practice, based in Ogden, Utah, provides gastroenterological medical services.

OCR began investigating Porter after it filed a breach report related to a dispute with a business associate. OCR's investigation determined that Porter had never conducted a risk analysis at the time it filed the breach report, and despite significant technical assistance throughout the investigation, had failed to complete an accurate and thorough risk analysis after the breach and failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

In addition to the monetary settlement, Porter agreed to:

- Complete an enterprise-wide risk analysis;
- Develop comprehensive policies and procedures to comply with the HIPAA Rules; and
- Train all workforce members who use or disclose PHI on revised policies and procedures.

This settlement occurred in February 2020. The resolution agreement is available at the following link: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/porter/index.html.

Resolution Agreement with Metropolitan Community Health Services dba Agape Health Services

Metropolitan Community Health Services doing business as Agape Health Services (Agape) agreed to pay $25,000 and take corrective action to settle potential violations of the HIPAA Security Rule. Agape is a Federally Qualified Health Center that provides a variety of discounted health services to the underserved population in rural North Carolina.

On June 9, 2011, Agape filed a breach report with OCR following discovery that a misdirected email transmission resulted in the compromise of the ePHI of 1,263 individuals. OCR's investigation revealed longstanding, systemic noncompliance with the HIPAA Security Rule. Specifically, Agape failed to conduct any risk analyses, failed to implement any HIPAA Security Rule policies and procedures, and neglected to provide workforce members with security awareness training until 2016.

[20] Information provided here on Resolution Agreements and CMPs are based on the year in which the Agreement was signed, or the CMP assessed. Investigations of these cases were initiated in years prior to 2020. No CMPs were assessed in 2020.

In addition to the monetary settlement, Agape agreed to:

- Complete an enterprise-wide risk analysis;
- Develop and implement risk management;
- Review and revise its written policies and procedures to comply with HIPAA Rules; and
- Train workforce members on the revised policies and procedures.

This settlement occurred in March 2020. The resolution agreement is available at the following link: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/metro/index.html.

Resolution Agreement with CHSPSC

CHSPSC, LLC agreed to pay $2,300,000 and adopt a corrective action plan to settle potential violations of the HIPAA Privacy and Security Rules. CHSPSC provides a variety of business associate services, including IT and health information management, to hospitals and physician clinics indirectly owned by Community Health Systems, Inc., in Tennessee.

In April 2014, the Federal Bureau of Investigation notified CHSPSC that it had traced a hacking group's advanced persistent threat to CHSPSC's information system. Despite this notice, the hackers continued to access and exfiltrate the ePHI of over 6.1 million individuals until August 2014. The hackers used compromised administrative credentials to remotely access CHSPSC's information system through its virtual private network.

OCR's investigation found longstanding, systemic noncompliance with the HIPAA Security Rule including failure to conduct a risk analysis, and failures to implement information system activity review, security incident procedures, and access controls.

In addition to the monetary settlement, CHSPSC agreed to:

- Conduct an enterprise-wide risk analysis;
- Develop and implement risk management;
- Revise its written policies and procedures to comply with the HIPAA Security Rule; and
- Train workforce members on revised HIPAA Security Rule policies and procedures.

This settlement occurred in March 2020. The resolution agreement is available at the following link: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/chspsc/index.html.

Resolution Agreement with Premera Blue Cross

Premera Blue Cross (PBC) agreed to pay $6.85 million and implement a corrective action plan to settle potential violations of the HIPAA Privacy and Security Rules. PBC operates in Washington and Alaska, and is the largest health plan in the Pacific Northwest, serving more than two million people.

On March 17, 2015, PBC filed a breach report on behalf of itself and its network of affiliates stating that cyber-attackers had hacked into its information technology system. The hackers used a phishing email to install malware that gave them access to PBC's IT system in May 2014, which went undetected for nearly nine months. This undetected attack resulted in the disclosure of more than 10.4 million individuals' ePHI including names, addresses, dates of birth, email addresses, Social Security numbers, financial information, and health plan clinical information.

OCR's investigation found systemic noncompliance with the HIPAA Rules including failure to conduct an enterprise-wide risk analysis, and failure to implement risk management and audit controls.

In addition to the monetary settlement, PBC agreed to:

- Conduct an enterprise-wide risk analysis;
- Develop and implement risk management; and
- Adopt and implement written policies and procedures to comply with the HIPAA Security Rule.

This settlement occurred in March 2020. The resolution agreement is available at the following link: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/premera/index.html.

Resolution Agreement with Lifespan Health System Affiliated Covered Entity

Lifespan Health System Affiliated Covered Entity (Lifespan) agreed to pay $1,040,000 and take corrective action to settle potential violations of the HIPAA Privacy and Security rules related to the theft of an unencrypted laptop. Lifespan is a non-profit health system based in Rhode Island.

OCR initiated its investigation after Lifespan filed a breach report on April 21, 2017 regarding the theft of an affiliated hospital employee's laptop containing ePHI that included the names, medical record numbers, demographic information, and medication information of 20,431 individuals. OCR's investigation determined that there was systemic noncompliance with the HIPAA Rules including a failure to encrypt ePHI on laptops after Lifespan determined it was reasonable and appropriate to do so. OCR also uncovered a lack of device and media controls, and a failure to have a business associate agreement in place with the Lifespan.

In addition to the monetary settlement, Lifespan agreed to:

- Develop policies and procedures to comply with the HIPAA Privacy and Security Rules;

- Provide written reporting to OCR pertaining to the encryption of devices that contain ePHI and have access to its network;
- Complete an accounting of business associate agreements between Lifespan and its affiliated healthcare providers; and
- Train all workforce members who have access to ePHI on its new policies and procedures.

This settlement occurred in June 2020. The resolution agreement is available at the following link: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/lifespan/index.html.

Resolution Agreement with Athens Orthopedic Clinic

Athens Orthopedic Clinic PA (Athens Orthopedic) agreed to pay $1,500,000 and adopt a corrective action plan to settle potential violations of the HIPAA Privacy and Security Rules. Athens Orthopedic is located in Georgia and provides orthopedic services to the local community.

On June 26, 2016, a journalist notified Athens Orthopedic that a database of their patient records may have been posted online for sale. A hacker subsequently contacted Athens Orthopedic and demanded money in return for a complete copy of the database it stole. Athens Orthopedic determined that the hacker used a vendor's credentials to access its electronic medical record system and exfiltrate patient health data. The hacker continued to access ePHI for over a month.

On July 29, 2016, Athens Orthopedic filed a breach report informing OCR that 208,557 individuals were affected by this breach, and that the ePHI disclosed included names, dates of birth, Social Security numbers, medical procedures, test results, and health insurance information.

OCR's investigation discovered longstanding, systemic noncompliance with the HIPAA Privacy and Security Rules including failures to conduct a risk analysis, implement risk management and audit controls, maintain HIPAA policies and procedures, secure business associate agreements with multiple business associates, and provide HIPAA Privacy Rule training to workforce members.

In addition to the monetary settlement, Athens Orthopedic agreed to:

- Conduct an enterprise-wide risk analysis;
- Develop and implement risk management;
- Adopt and implement written policies and procedures to comply with the HIPAA Privacy and Security Rules;
- Train workforce members on HIPAA Privacy and Security Rule policies and procedures; and
- Identify all business associates and provide copies of business associate agreements.

This settlement occurred in July 2020. The resolution agreement is available at the following link: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/athens-orthopedic/index.html.

Resolution Agreement with Aetna Life Insurance Company

Aetna Life Insurance Company and the affiliated covered entity (Aetna) agreed to pay $1,000,000 and adopt a corrective action plan to settle potential violations of the HIPAA Privacy and Security Rules. Aetna is an American managed health care company that sells traditional and consumer-directed health insurance and related services.

In June 2017, Aetna submitted a breach report to OCR stating that on April 27, 2017, Aetna discovered that two web services used to display plan-related documents to health plan members allowed documents to be accessible and subsequently indexed by various internet search engines. Aetna reported that 5,002 individuals were affected by this breach, and the PHI disclosed included names, insurance identification numbers, claim payment amounts, procedure service codes, and dates of service.

In August 2017, Aetna submitted another breach report to OCR stating that on July 28, 2017, benefit notices were mailed to members using window envelopes which exposed individuals' PHI. Aetna reported that 11,887 individuals were affected by this impermissible disclosure.

In November 2017, Aetna submitted another breach report to OCR stating that on September 25, 2017, a research study mailing sent to Aetna plan members exposed individuals' PHI. Aetna reported that 1,600 individuals were affected by this impermissible disclosure.

OCR's investigation revealed that in addition to the impermissible disclosures, Aetna failed to perform periodic technical and nontechnical evaluations of operational changes affecting the security of their ePHI; implement procedures to verify the identity of persons or entities seeking access to ePHI; limit PHI disclosures to the minimum necessary to accomplish the purpose of the use or disclosure; and have in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI.

In addition to the monetary settlement, Aetna agreed to:

- Adopt and implement written policies and procedures to comply with the HIPAA Privacy and Security Rules; and
- Train all workforce members who have access to PHI on revised policies and procedures.

This settlement occurred in October 2020. The resolution agreement is available at the following link: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/aetna/index.html.

Resolution Agreement with City of New Haven

The City of New Haven, Connecticut (New Haven) agreed to pay $202,400 and implement a corrective action plan to settle potential violations of the HIPAA Privacy and Security Rules. The New Haven Health Department (NHHD), among other things, operates a public health clinic that provides preventative medical services, including adult and pediatric immunizations.

In January 2017, NHHD filed a breach report with OCR stating that a former employee may have accessed a file on a New Haven computer containing the PHI of 498 individuals. OCR's investigation revealed that, on July 27, 2016, a former employee returned to NHHD, eight days after being terminated, logged into her old computer with her still-active user name and password, and downloaded PHI that included names, addresses, dates of birth, race/ethnicity, gender, and sexually transmitted disease test results onto a USB drive. Additionally, OCR found that the former employee had shared her user ID and password with an intern, who continued to use these login credentials to access PHI on NHHD's network after the employee was terminated.

OCR's investigation determined that NHHD failed to conduct an enterprise-wide risk analysis, and failed to implement termination procedures, access controls such as unique user identification, and HIPAA Privacy Rule policies and procedures.

In addition to the monetary settlement, New Haven agreed to:

- Conduct an enterprise-wide risk analysis;
- Develop and implement risk management;
- Adopt and implement written policies and procedures to comply with the HIPAA Privacy and Security Rules; and
- Train workforce members on HIPAA Privacy and Security Rule policies and procedures.

This settlement occurred in October 2020. The resolution agreement is available at the following link: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/new-haven/index.html.