Annual Report to Congress on Breaches of Unsecured Protected Health Information

For Calendar Year 2022

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 Health Insurance Portability and Accountability Act of 1996 (HIPAA) enforcement activities undertaken by the United States Department of Health and Human Services (HHS), Office for Civil Rights (OCR) during the 2022 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 626 notifications [1] of breaches affecting 500 or more individuals, representing an increase of 3% from the number of reports received in calendar year 2021. These reported breaches affected a total of approximately 41,747,613 individuals. The most commonly reported category of breaches was hacking, and the largest breach of this type involved approximately 3,300,638 individuals. OCR also received 63,966 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 257,105 individuals.

OCR initiated investigations into all 626 breaches affecting 500 or more individuals, as well as two breaches involving fewer than 500 individuals. OCR completed 799 breach investigations through the provision of technical assistance, achieving voluntary compliance through corrective action, resolution agreements and corrective action plans, or after determining no violation occurred. Specifically, OCR resolved three breach investigations with resolution agreements, corrective action plans, and monetary payments totaling $2,425,640.[2]

Recommendations

There is a continued need for regulated entities to improve compliance with the HIPAA Rules. In particular, the Security Rule standards [3] and implementation specifications[4] of risk analysis, risk management, information system activity review, audit controls, response and reporting, and person or entity authentication were areas identified as needing improvement in 2022 OCR breach investigations.

As in previous years, hacking/IT incidents remained the largest category of breaches affecting 500 or more individuals occurring in 2022, comprising 74% of the reported breaches. Hacking/IT

[1] This figure reflects the number of breaches affecting 500 or more individuals that occurred or ended in calendar year 2022. In total, OCR received 717 breach reports via the HIPAA Breach Web Portal in 2022, but some of these breaches did not occur in 2022 (e.g., breach occurred in 2021, and was reported to OCR in 2022).

[2] The three breach investigations resolved in 2022 were Oklahoma State University - Center for Health Sciences, New England Dermatology dba New England Dermatology and Laser Center, and Banner Health.

[3] *Standard* means a rule, condition, or requirement: (1) Describing the following information for products, systems, services, or practices: (i) Classification of components; (ii) Specification of materials, performance, or operations; or (iii) Delineation of procedures; or (2) With respect to the privacy of protected health information. 45 CFR 160.103 definition of "standard".

[4] *Implementation specification* means specific requirements or instructions for implementing a standard. 45 CFR 160.103 definition of "implementation specification".

incidents also affected the most individuals (32,255,597). The largest category of breaches of 500 or more individuals by location was network servers. For breaches affecting fewer than 500 individuals, the largest category by type of breach report was unauthorized access or disclosures, and the largest category by location was paper records.

Background

The HIPAA Privacy Rule, found at 45 CFR Part 160 and Subparts A and E of Part 164, 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.

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 under HIPAA to notify affected individuals, the Secretary of Health and Human Services ("the Secretary"), and, in some cases, the media, following the discovery of a breach of unsecured PHI. Business associates under HIPAA are required to notify covered entities following the discovery of a breach of unsecured PHI.

Section 13402(i) of the HITECH Act requires 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 2022.

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.[5] 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."

HHS promulgated a final rule regarding Breach Notification for Unsecured Protected Health Information on January 25, 2013 (78 FR 5566).

OCR is the office within HHS that is responsible for administering and enforcing the HIPAA

[5] https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html.

Privacy, Security, and Breach Notification Rules.

Definition of Breach

Consistent with the definition of breach in section 13400(1)(A) of the HITECH Act, HHS defines "breach" at 45 C.F.R. § 164.402 as the "acquisition, access, use, or disclosure of PHI in a manner not permitted by [the HIPAA Privacy Rule] 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.[6]

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 C.F.R. § 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 atthe 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 notificationof 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.[7] These breach notification requirements for covered entities and business associates are set forth at 45 CFR §§ 164.404 – 164.410.

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

[7] 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 or which party 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 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.[8]

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. As with 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.[9]

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. [10] 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

[8] *See* 45 CFR § 164.404.
[9] *See* 45 CFR § 164.406.
[10] *See* 45 CFR § 164.408(b).

the breaches were discovered.[11] Covered entities must notify the Secretary by filling out and electronically submitting a breach report form on the HHS website at https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.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 (when applicable) 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.[12]

Investigations

When OCR initiates an investigation based upon the receipt of a breach report, OCR collects evidence through interviews, witness statements, requests for data from the entity involved, site visits, or other available, relevant documents.

In some cases, OCR may determine, based on the evidence, that there is insufficient evidence to support a finding that a covered entity or business associate violated the HIPAA Rules. In such cases, OCR sends a closure letter to the parties involved explaining the results of the investigation.

In other cases, OCR may determine, based on the evidence, that the covered entity or business associate was not in compliance with the HIPAA Rules. In such cases, OCR will generally first attempt to resolve the case by obtaining compliance through corrective action, which may include a resolution agreement.

Where corrective action is sought, OCR obtains satisfactory documentation and other evidence from the covered entity or business associate that it undertook the required corrective action to resolve the potential HIPAA violation(s). In the vast majority of cases, a covered entity or business associate will, through cooperation and corrective action, be able to demonstrate satisfactory compliance with the HIPAA Rules.

Resolution Agreements

Where OCR finds indications of noncompliance due to willful neglect, or where the nature and scope of the noncompliance warrants additional enforcement action, OCR pursues a resolution

[11] *See* 45 CFR § 164.408(c).

[12] 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.

agreement with a payment of a settlement amount and an obligation to complete a corrective action plan (CAP). In these cases, OCR notifies the covered entity or business associate that, while OCR is prepared to assess a CMP with regard to the potential violations of the HIPAA Rules, OCR is willing to negotiate the terms of a resolution agreement and CAP to informally resolve the indications of noncompliance. These settlement agreements involve the payment of a monetary amount that is a reduced percentage of the potential CMP for which the covered entity or business associate could be liable. Additionally, in most cases, the resolution agreement includes a CAP that requires the covered entity or business associate to fix remaining compliance issues and to undergo OCR monitoring of its compliance with the HIPAA Rules for a specified time. While this type of resolution still constitutes informal enforcement action on the part of OCR, resolution agreements and CAPs are powerful enforcement tools for OCR as they address noncompliance and deter future noncompliance with the HIPAA Rules for entities under investigation, and when OCR announces those resolutions, the announcements serve as reminders to the wider regulated community of their own HIPAA obligations.

Civil Money Penalties

If OCR and a covered entity or business associate are unable to reach a satisfactory agreement to resolve the matter informally, or if a covered entity or business associate breaches the terms of a resolution agreement, OCR may pursue formal enforcement. In such cases, OCR notifies the covered entity or business associate of a proposed determination of a violation of the HIPAA Rules and OCR's intent to impose a CMP. If a CMP is proposed, the covered entity or business associate may request a hearing in which the Departmental Appeals Board decides if the CMP is supported by the evidence in the case. If the covered entity or business associate does not request a hearing within 90 days of receipt of OCR's proposed determination, OCR will issue a final determination and impose a CMP.

Summary of Breach Reports

This report describes the types and numbers of breaches reported to OCR that occurred between January 1, 2022, and December 31, 2022, and describes actions 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 2022.* 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 2022, in addition to requiring covered entities and business associates to take corrective action in hundreds of cases, OCR resolved three breach investigations with resolution agreements, corrective action plans, and monetary payments totaling $2,425,640.

As shown in the table below, the number of breaches reported to OCR continues to increase. Between 2018 and 2022, the number of breaches affecting fewer than 500 individuals increased 1% and the number of breaches affecting 500 or more individuals rose 107%.

Year	Under500 Breaches Reported	500+ Breaches Reported	Percentage Change in Under 500 Breaches Reported	Percentage Change in 500+Breaches Reported
2022	63,966	626	**1%** increase	3% increase
2021	63,571	609	-4% decrease	-7% decrease
2020	66,509	656	6% increase	61% increase
2019	62,771	408	-.5% decrease	35% increase
2018	63,098	302		
2018 to 2022	1.4% increase	107% increase		

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 626 reports of such breaches for calendar year 2022,[13] which affected a total of approximately 41,747,613 individuals.[14]

Breaches in 2022 Affecting 500 or More Individuals[15]

For the 626 breaches affecting 500 or more individuals in 2022, OCR received:

(1) 425 reports (68%) of breaches from health care providers (affecting 24,481,253 individuals (59%));

[13] HHS 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 2020 into 2022 would be reported with the 2022 figures).

[14] 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.

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

(2) 120 reports (19%) of breaches from business associates (affecting 14,580,712 individuals (35%));

(3) 80 reports (13%) of breaches from health plans (affecting 2,683,148 individuals (6%)); and

(4) 1 report (<1%) of breaches from health care clearinghouses (affecting 2,500 individuals (<1%)).

See Figures 1 and 2.

HHS Office for Civil Rights
Breach Reports of Unsecured PHI Affecting 500 or more Individuals in 2022 by Percentage of Reports Received by Entity Type

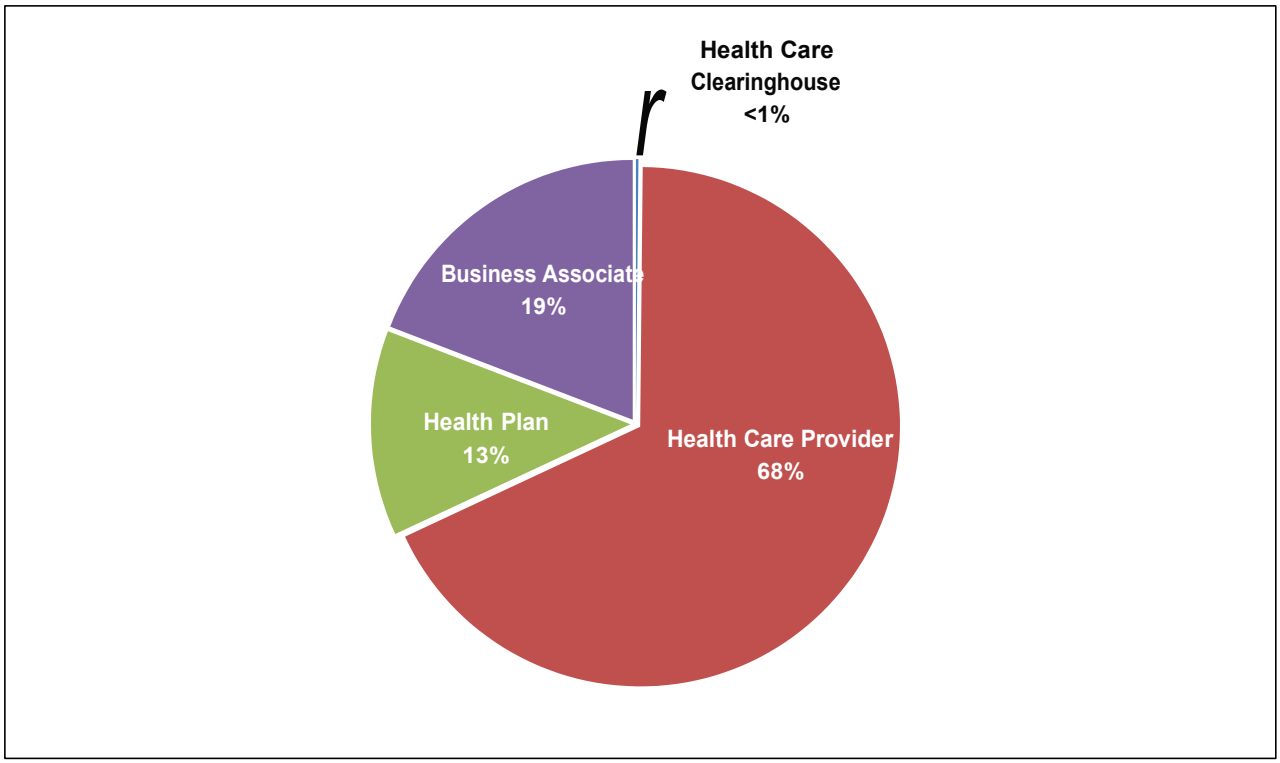

Figure 1

HHS Office for Civil Rights
Breach Reports of Unsecured PHI Affecting 500 or more Individuals in 2022 by Percentage of Individuals Affected by Entity Type

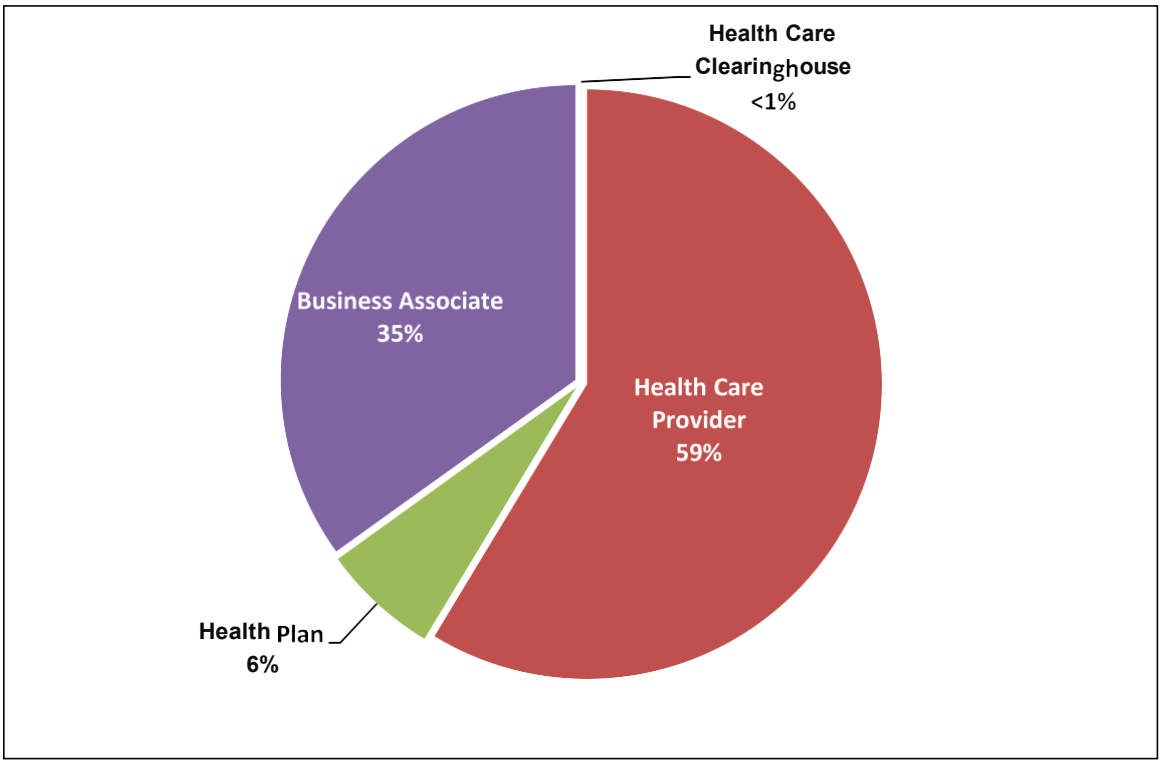

Figure 2

The 626 reports submitted to OCR for breaches affecting 500 or more individuals occurring in 2022 can be categorized by five general types or causes as follows (in order of frequency):[16]

(1)) Hacking/IT incident of electronic equipment or a network server (462 reports (74%) affecting 32,255,597 individuals (77%));

(2) Unauthorized access or disclosure ofrecords containing PHI (122 reports (19%) affecting 9,030,525 individuals (22%));

(3) Theft of electronic equipment/portable devices or paper containing PHI (28 reports (4%) affecting 433,155 individuals (1%));

(4) Loss of electronic media or paper records containing PHI (11 reports (2%) affecting 15,665 individuals (<1%)); and

(5) Improper disposal of PHI (3 reports (<1%) affecting 12,671 individuals (<1%)).

See Figures 3 and 4.

[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 500 or more Individuals in 2022
by Percentage of Reports Received
by Type of Breach

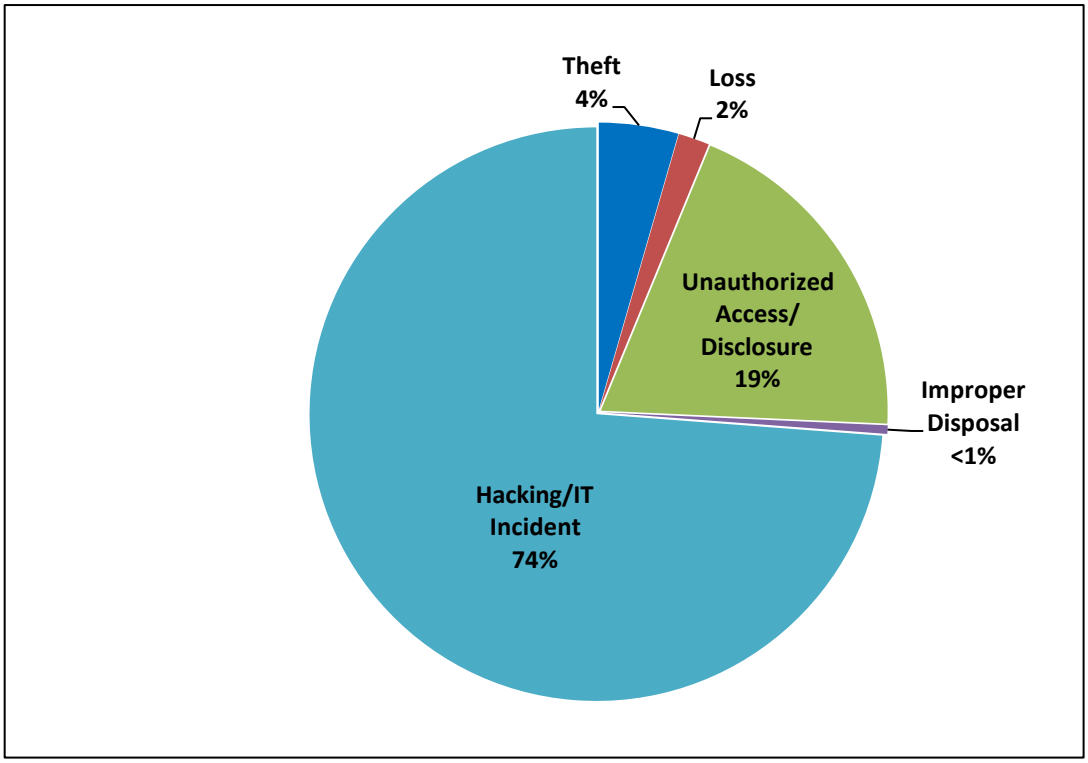

Figure 3

HHS Office for Civil Rights
Breach Reports of Unsecured PHI Affecting 500 or more Individuals in 2022
by Percentage of Individuals Affected
by Type of Breach

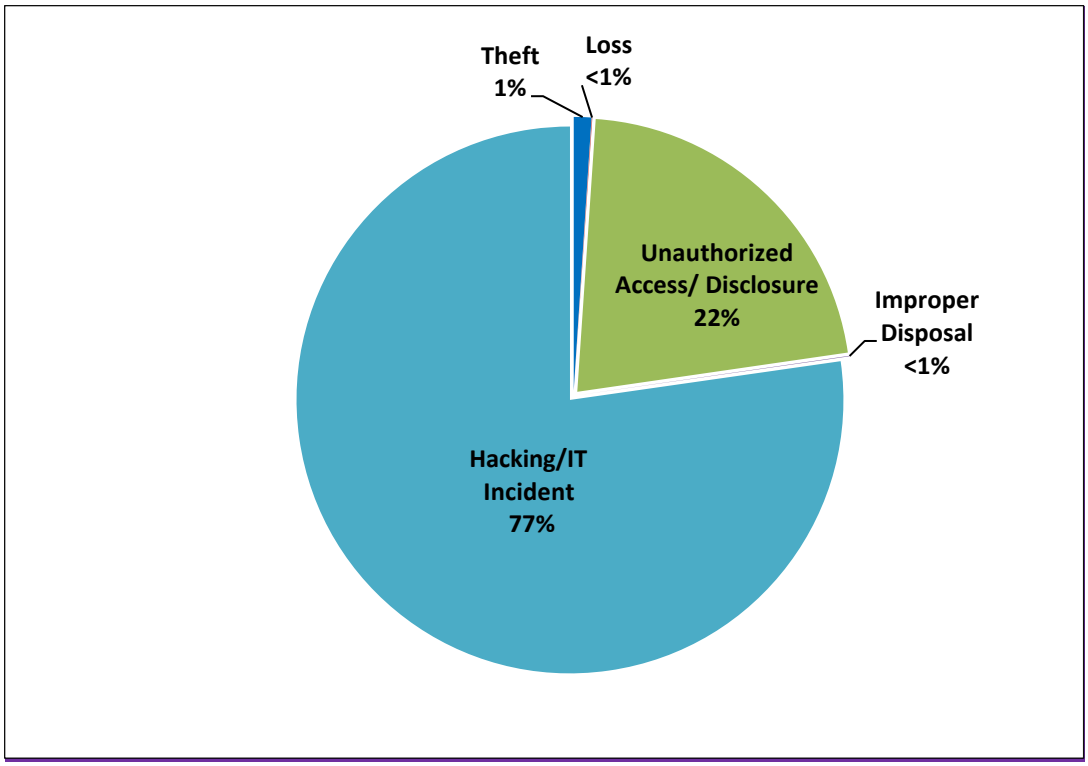

Figure 4

The 626 reports submitted to OCR for breaches occurring in 2022 described the following locations of the PHI (in order of frequency):[17]

(1) Network server (364 reports (58%) affecting 32,936,422 individuals (79%));
(2) E-mail (136 reports (22%) affecting 2,337,032 individuals (6%));
(3) Paper (37 reports (6%) affecting 303,006 individuals (1%));
(4) Electronic medical record (35 reports (6%) affecting 4,671,468 individuals (11%));
(5) Desktop computer (24 reports (4%) affecting 1,235,927 individuals (3%))
(6) Other portable electronic device (17 reports (3%) affecting 201,879 individuals (<1%));
(7) Laptop computer (12 reports (2%) affecting 61,288 individuals (< 1%)); and
(8) Other (1 report (<1%) affecting 591 individuals (<1%)).[18]

See Figures 5 and 6.

[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] 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.

HHS Office for Civil Rights
Breach Reports of Unsecured PHI Affecting 500 or more Individuals in 2022 by Percentage of Reports Received by Location of PHI

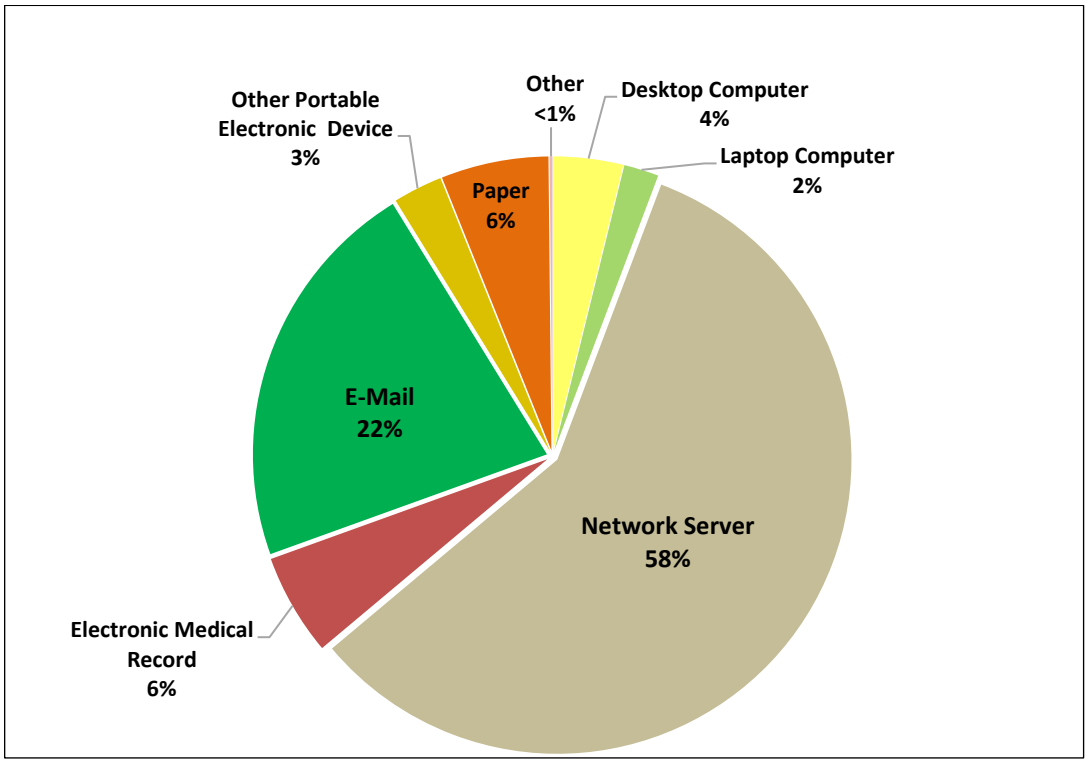

Figure 5

HHS Office for Civil Rights
Breaches of Unsecured PHI affecting 500 or More Individuals in 2022
by Percentage of Individuals Affected
by Location of PHI

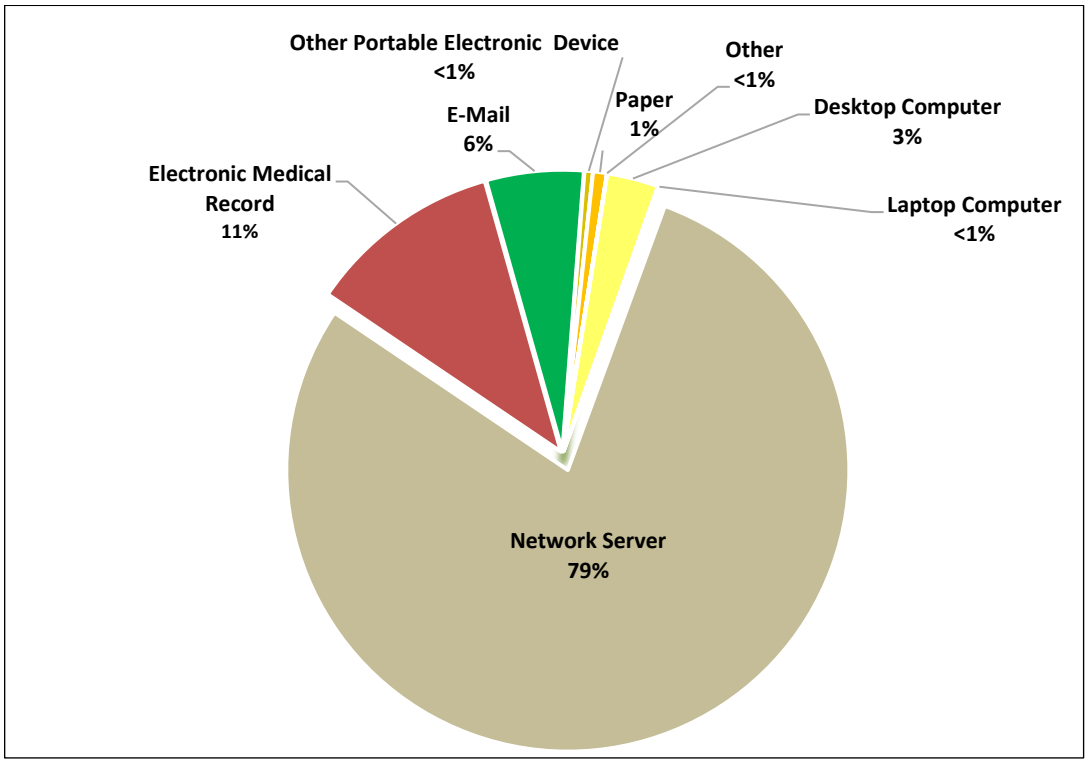

Figure 6

Largest breaches in 2022 for each reported cause

This section describes the largest breaches, 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 2022 resulted from a hacking/IT incident in which hackers deployed ransomware that compromised the servers of a healthcare provider containing ePHI. The breach incident affected 3,388,856 individuals. Other hacking/IT incidents involved the use of malware, phishing, and the posting of PHI to public websites.

Unauthorized Access or Disclosure of PHI: The largest breach in 2022 involving the unauthorized access or disclosure of ePHI affected approximately 3,000,000 individuals. In this case, a healthcare provider reported that it used data tracking technologies in a manner that resulted in the impermissible disclosure of ePHI to tracking technology vendors. Other incidents of unauthorized access or disclosure involved the posting of ePHI to public websites accessible via the Internet, employees impermissibly accessing records outside the scope of their job responsibilities, and misdirected communications.

Improper Disposal: The largest reported improper disposal incident in 2022 resulted from a business associate who improperly disposed of paper medical records by throwing them away

in a dumpster. This breach affected approximately 7,500 individuals. Most improper disposal breaches involved disposing of paper records containing PHI in trash bins rather than authorized shred bins or another secure disposal method.

Theft: The largest theft-related breach in 2022 resulted from the theft of paper medical records when a storage facility was burglarized and six boxes containing medical records were stolen. The theft affected approximately 149,940 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 2022 resulted from the loss of medical records via a pipe that broke and damaged the medical records of approximately 2,500 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 2022, 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 analysis; 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 2022, notification to OCR was required no later than March 1, 2023.

Breaches involving fewer than 500 individuals for 2022

OCR received 63,966 reports of breaches affecting fewer than 500 individuals occurring in calendar year 2022. These smaller breaches affected 257,105 individuals. Set forth below are the breaches submitted to OCR by covered entity type (in order of frequency):

(1) Health Care Providers (58,504 reports (91%) affecting 188,167 individuals (73%));

(2) Health Plans (3,651 reports (6%) affecting 38,122 individuals (15%));

(3) Business Associates (1,746 reports (3%) affecting 30,106 individuals (12%)); and

(4) Health Care Clearinghouses (65 reports (<1%) affecting 710 individuals (<1%)).

See Figures 7 and 8.

HHS Office for Civil Rights
Breach Reports of Unsecured PHI affecting Fewer Than 500 Individuals in 2022 by Percentage of Reports Received by Entity Type

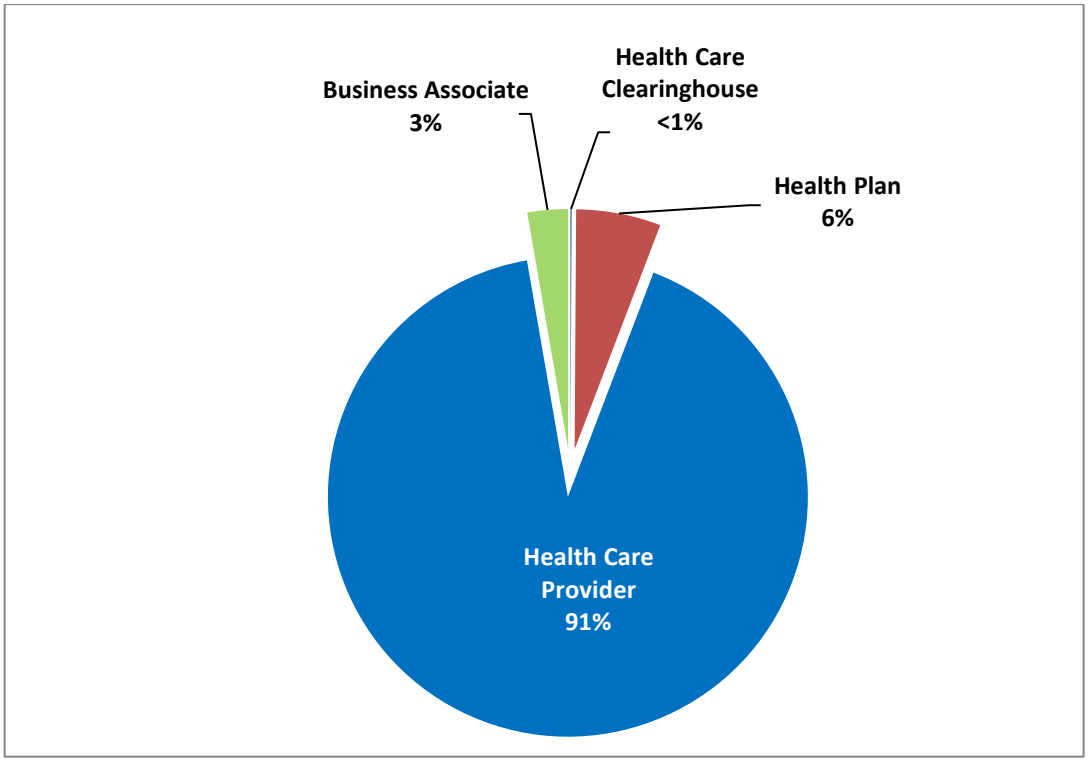

Figure 7

HHS Office for Civil Rights
Breach Reports of Unsecured PHI affecting Fewer Than 500 Individuals in 2022 by Percentage of Individuals Affected by Entity Type

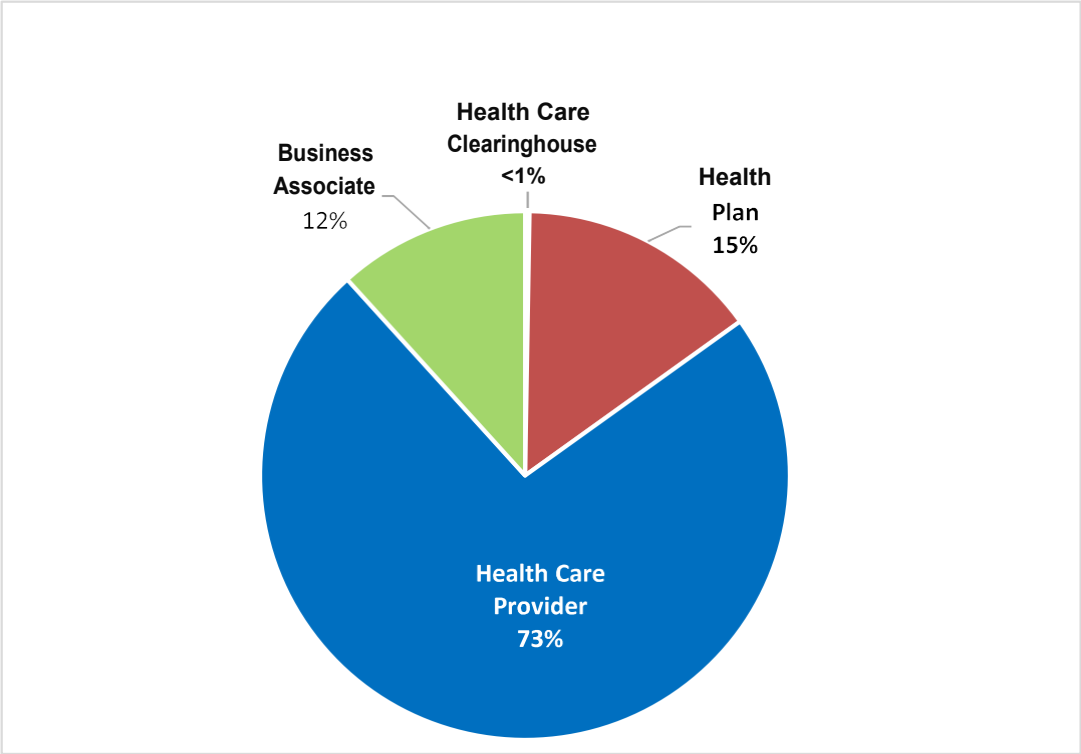

Figure 8

The most common causes or types of breach incidents (in order of frequency) for breaches affecting fewer than 500 individuals were:[19]

(1) Unauthorized access or disclosure (59,727 reports (93%) affecting 171 ,100 individuals (67%));

(2) Loss (2,383 reports (4%) affecting 9,989 individuals (4%));

(3) Theft (859 reports (1%) affecting 20,568 individuals (8%));

(4) Hacking/IT incident (822 reports (1%) affecting 50,099 individuals (19%)); and

(5) Improper disposal (175 reports (<1%) affecting 5,349 individuals (2%)).

See Figures 9 and 10.

[19] 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 2022 by Percentage of Reports Received
by Type of Breach

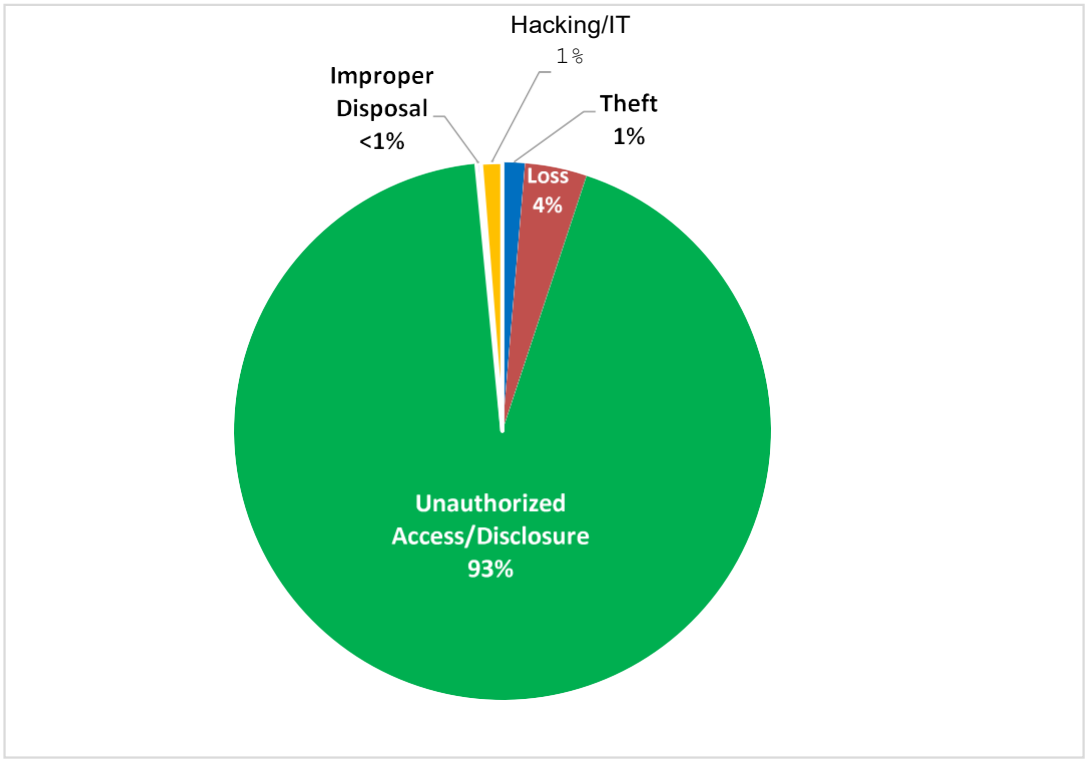

Figure 9

HHS Office for Civil Rights
Breach Reports of Unsecured PHI affecting Fewer Than 500 Individuals in 2022 by Percentage of Individuals Affected by Type of Breach

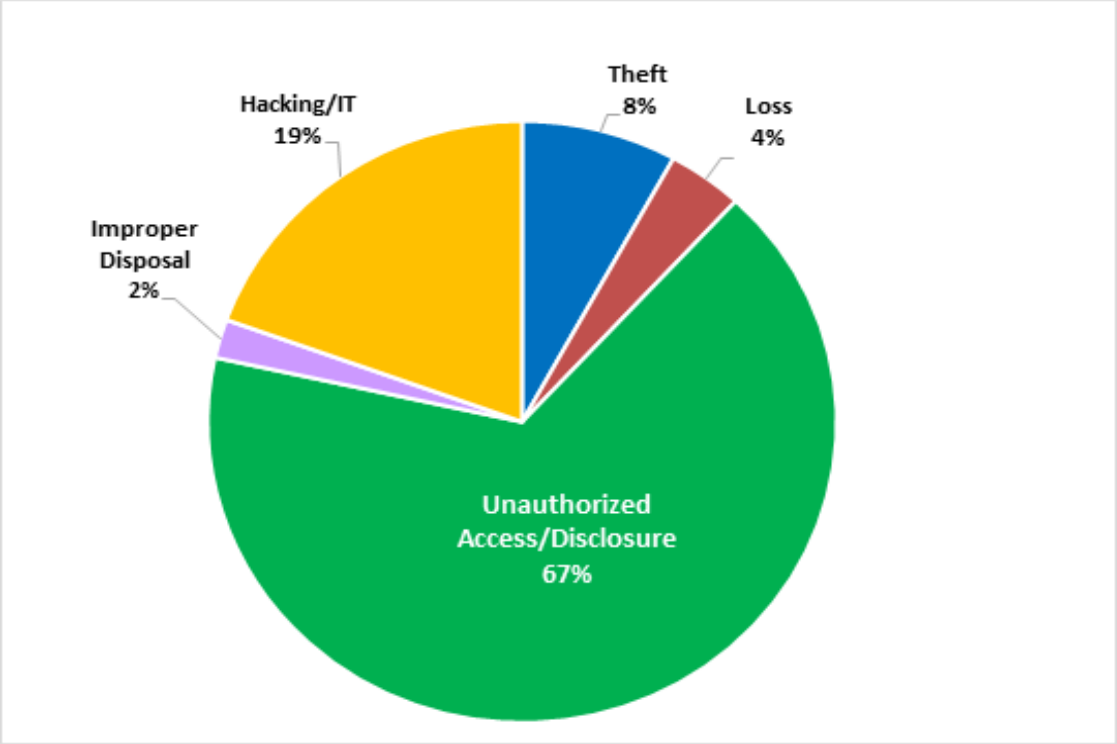

Figure 10

The 63,966 reported breaches affecting fewer than 500 individuals described the following locations of the PHI (in order of frequency):[20]

(1) Paper (39,595 reports (62%) affecting 85,363 individuals (33%));
(2) Electronic medical record (EMR) (10,862 reports (17%) affecting 35,521 individuals (14%));
(3) Other (7,381 reports (12%) affecting 33,080 individuals (13%));[21]
(4) E-mail (3,731 reports (6%) affecting 50,935 individuals (20%));
(5) Other portable electronic device (801 reports (1%) affecting 3,981 individuals (2%));
(6) Desktop computer (785 reports (1%) affecting 8,408 individuals (3%));
(7) Network server (589 reports (1%) affecting 31,488 individuals (12%)); and
(8) Laptop computer (222 reports (< 1%) affecting 8,329 individuals (3%)).

See Figures 11 and 12.

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

HHS Office for Civil Rights
Breach Reports of Unsecured PHI affecting Fewer Than 500 Individuals in 2022 by Percentage of Reports Received by Location of Breach

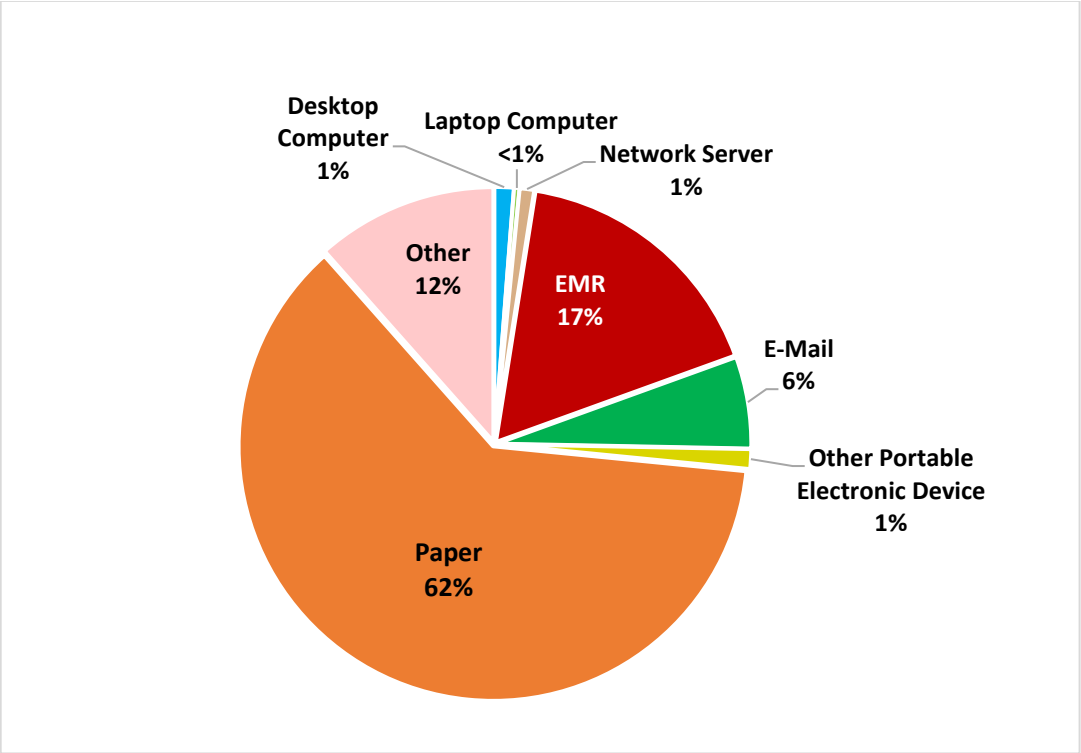

Figure 11

HHS Office for Civil Rights
Breaches of Unsecured PHI affecting Fewer Than 500 Individuals in 2022 by Percentage of Individuals Affected by Location of PHI

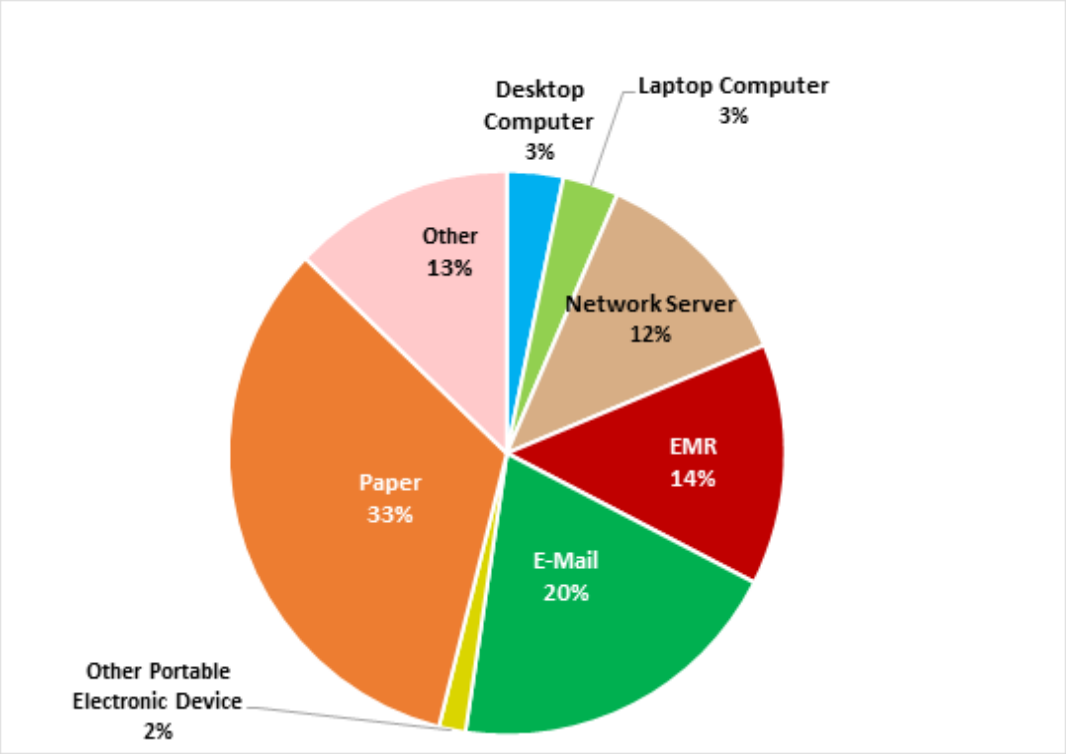

Figure 12

Details on breaches involving fewer than 500 individuals for 2022

As in previous years, breach incidents reported for 2022 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 2022 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.

OCR completed 21 breach investigations involving fewer than 500 individuals in 2022.

Cases Investigated and Action Taken

OCR opened investigations into all 626 reported breaches affecting 500 or more individuals that

occurred in 2022. OCR also opened 2 investigations into breaches affecting fewer than 500 individuals. OCR completed 799 breach investigations through the provision of technical assistance, achieving voluntary compliance through corrective action, resolution agreements and corrective action plans , or after determining no violation occurred. Specific details about the cases that were resolved in 2022 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 Compliancefor Calendar Year 2022.*

Lessons Learned

The breach reports submitted to OCR offer insight into common deficiencies and vulnerabilities in protections for the privacy and security of individuals ' PHI. The following HIPAA Security Rule standards and implementation specifications were identified in OCR investigations in 2022 as areas needing improvement:

- Security Management Process Standard. [22] The Security Rule requires regulated entities to implement policies and procedures to prevent, detect, contain, and correct security violations. Specific implementation specifications within this administrative safeguard standard needing improvement include:
    - Risk Analysis. [23] The Security Rule requires regulated entities to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentia lity, integrit y, and availability of all ePHI held by the covered entity or business associate. Security Rule investigations in 2022 found numerous instances where regulated entities ' risk analyses lacked a comprehensive understanding of the potential risks and vulnerabilities to ePHI in their environments. Specifically, the risk analyses , if conducted at all, were often based on incomplete inventories of where PHI is created, received , maintained or transmitted, resulting in an incomplete assessment of risks and vulnerabilities that is deficient in scope. Failures to conduct an accurate and thorough risk analysis leave regulated entities vulnerable to breaches of unsecured ePHI as cybersecurity attacks are increasing.
    - Risk Management. [24] The Security Rule requires regulated entities to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. OCR' s investigations continued to identify noncompliance with these requirements including failures to implement security measures to reduce the same risks identified repeatedly over a protracted period of time. Failures to implement risk management leave regulated entities vulnerable to breaches of unsecured ePHI as cybersecurity attacks are increasing .
    - Information System Activity Review. [25] The Security Rule requires regulated entities to regularly review records of information system activity, such as

[22] 45 C.F.R. §164.308(a)(l).
[23] 45 C.F.R. §164.308(a)(l)(ii)(A).
[24] 45 C.F.R. §164.308(a)(l)(ii)(B).
[25] 45 C.F.R. §164.308(a)(l)(ii)(D).

audit logs, access reports, and security incident tracking reports. OCR's investigations in 2022 continued to find instances of deficient or non-existent information system activity review processes. Examples of deficient processes include a total lack of review of information system activity as well as reviews that were ad hoc, reactive or deficient in scope which leaves access to some PHI unmonitored. A successful system activity review process can play a critical role in detecting malicious activity, including from malicious insiders. Early detection of malicious activity can be key to eliminating or mitigating potential breaches and reducing the potential number of individuals affected.

- Audit Controls Standard. [26] The Security Rule requires regulated entities to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI. Audit controls record and can help detect suspicious activity that may indicate information systems have been compromised and can also be reviewed to identify malicious activity that previously occurred. Maintaining robust audit controls can be important to understand how attackers gained access to information systems and help identify the scope of malicious actions. OCR's investigations continued to find regulated entities that either do not have such mechanisms in place or have implemented audit control mechanisms for only a narrow subset of its systems containing or using ePHI. In other cases, entities have deficient logging procedures that fail to maintain access or activity logs for a practicable amount of time *(e.g.,* logs are not maintained for review). Failure to comply with the Security Rule ' s audit controls requirement reduces the visibility of potential malicious activity which can delay security incident responses and investigations.

- Response and Reporting. [27] The Security Rule requires regulated entities to identify and respond to suspected or known security incidents , mitigate to the extent practicable, harmful effect of security incidents that are known to the regulated entity, and document security incidents and their outcomes. OCR' s investigations found instances of deficient or non-existent security incident response and reporting processes. Regulated entities that do not effectively respond to security incidents , including breaches of ePHI, risk prolonging the harmful effects of security incidents and may even permit future security incidents by not identifying and mitigating the full breadth and depth of malicious actions. Swift and effective security incident response can reduce the impact of security incidents by expediting recovery times and reducing potential compromises of ePHI. In addition, OCR has discovered that regulated entities are frequently not documenting security incidents and their outcomes. Not only is this documentation specifically required in the Security Rule, but it is also crucial for an entity to maintain a record of the details of any security incident and the responsive steps taken for future reference, including relevant dates, staff members involved, systems affected, and any technical changes employed.

- Person or Entity Authentication.[28] The Security Rule requires regulated entities to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed. The use of compromised credentials is one of the leading methods attackers leverage to gain unauthorized access to an organization's network and

[26] 45 C.F.R. §164.312(b).
[27] 45 C.F.R. §164.308(a)(6)((ii).
[28] 45 C.F.R. §164.312(d).

information systems. OCR's investigations found instances of ineffective authentication procedures including weak password rules, using User IDs as passwords, sharing login credentials, and not changing application default passwords. Strong authentication is often the first line of defense to protect against cyber-attacks and potential breaches of ePHI.

Summary and Conclusion

The number of breaches experienced by regulated entities continues to rise and hacking/IT incidents remains the largest category of breaches of unsecured PHI affecting 500 or more individuals, at 74% of the reports received and 77% of the individuals affected in 2022. Health care providers experienced the majority of these (68%), which affected over 24.4 million individuals. Network servers remained the largest category by location for breaches affecting 500 or more individuals. For the breaches affecting fewer than 500 individuals that occurred in 2022, unauthorized access or disclosure was the largest category of type of breach reported (93%), and paper records was the largest by location (62%).

The breach notification requirements increase transparency of breaches both with the public at-large and within the regulated industry, as well as promotes accountability of covered entities and business associates. The reports submitted to OCR show that millions of affected individuals are receiving notifications of breach incidents in a timely fashion. As required by Section 13402(e)(4) of the HITECH Act, and 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 breach report investigations 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 affecting 500 or more individuals, as well as into select breaches affecting fewer than 500 individuals. During 2022, OCR resolved three breach investigations with resolution agreements/corrective action plans and collected settlements totaling over $2.4 million.[29]

[29] The three cases were Oklahoma State University - Center for Health Sciences, New England Dermatology dba New England Dermatology and Laser Center, and Banner Health.

APPENDIX

Resolution Agreements[30] in 2022

Resolution Agreement with Oklahoma State University- Center for Health Sciences

Oklahoma State University - Center for Health Sciences (OSU-CHS) paid $875,000 and agreed to take corrective action to settle potential violations of the HIPAA Privacy, Security, and Breach Notification Rules. OSU-CHS is a public land-grant research facility that provides preventative, rehabilitation, and diagnostic care in Oklahoma.

OCR began investigating OSU-CHS after it filed a breach report stating that an unauthorized third party had gained access to a web server that contained electronic PHI. The hackers installed malware that ultimately resulted in the impermissible disclosure of the PHI of 279,865 individuals. OCR' s investigation found potential violations of the HIPAA Rules including impermissible uses and disclosures of PHI, failure to conduct an accurate and thorough risk analysis, failure to implement audit controls, failure to provide security incident response and reporting, and failure to provide timely breach notification to affected individuals and HHS.

In addition to the monetary settlement, OSU-CHS agreed to:

- Conduct a comprehensive and thorough risk analysis;
- Develop an enterprise-wide Risk Management Plan to address and mitigate security risks and vulnerabilities found in the risk analysis;
- Develop, maintain, and revise, as necessary its written policies and procedures to comply with the HIPAA Rules;
- Distribute policies and procedures to workforce members; and
- Train workforce members on the policies and procedures for the privacy and security of PHI.

This settlement occurred in May 2022. The resolution agreement is available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreement/sosu/index.html.

Resolution Agreement with New England Dermatology dba New England Dermatology & Laser Center

New England Dermatology, P.C. dba New England Dermatology and Laser Center (NEDLC) paid $300,640 and agreed to adopt a corrective action plan to settle a potential violation of the HIPAA Privacy Rule. NEDLC is located in Massachusetts and provides dermatology services.

OCR began investigating NEDLC after it filed a breach report stating that empty specimen containers with PHI on the labels were placed in garbage bins located in the parking lot. In its investigation, OCR found potential violations of the HIPAA Privacy Rule including the impermissible use and disclosure of PHI and failure to maintain appropriate safeguards to protect the privacy of PHI.

[30] 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 2022.

In addition to the monetary settlement, NEDLC agreed to:

- Develop, maintain, and revise, as necessary its written policies and procedures to comply with the HIPAA Privacy Rule;
- Distribute policies and procedures to workforce members; and
- Train workforce members on the policies and procedures for the privacy of PHI.

This settlement occurred in July 2022. The resolution agreement is available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/nedlc/index.html.

Resolution Agreement with Banner Health

Banner Health Affiliated Covered Entities (Banner Health) paid $1,250,000 and agreed to take corrective action to settle potential violations of the HIPAA Security Rule. Banner is a nonprofit health system headquartered in Phoenix, Arizona.

OCR began investigating Banner after it filed a breach report stating that a threat actor had gained unauthorized access to ePHI. The hackers were able to gain access to the PHI of 2.81 million individuals. OCR's investigation found potential violations of the HIPAA Rules including failures to: conduct an accurate and thorough risk analysis, regularly review records of information system activity, implement procedures to verify that a person or entity seeking access to ePHI is the one claimed, and implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.

In addition to the monetary settlement, Banner agreed to:

- Conduct a comprehensive and thorough risk analysis;
- Develop an enterprise-wide risk management plan to address and mitigate security risks and vulnerabilities found in the risk analysis;
- Develop, maintain, and revise, as necessary its written policies and procedures to comply with the HIPAA Rules; and
- Distribute policies and procedures to workforce members.

This settlement occurred in December 2022. The resolution agreement is available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/banner-health/index.html.