Annual Report to Congress on Breaches of Unsecured Protected Health Information

For Calendar Year 2023

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 2023 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 (the Secretary) during the year and the actions taken in response to those breaches.

Summary

OCR received 732 notifications[1] of breaches of unsecured PHI affecting 500 or more individuals that occurred during 2023, representing an increase of 17% from the number of reports received in calendar year 2022. These reported breaches affected a total of approximately 113,173,613 individuals. The most commonly reported category of breaches was hacking, and the largest breach of this type involved approximately 11,270,000 individuals. OCR also received 68,315 reports[2] of breaches affecting fewer than 500 individuals that occurred during 2023, with unauthorized access or disclosure as the most frequent type of breach reported. These smaller breaches affected a total of 269,290 individuals.

OCR initiated investigations into all of the reported breaches of unsecured PHI affecting 500 or more individuals, as well as nine reported breaches affecting fewer than 500 individuals. OCR completed and resolved 724 breach investigations through the provision of technical assistance, achieving compliance through corrective action, resolution agreements and corrective action plans, or after determining no violation occurred. Specifically, OCR resolved seven breach investigations with resolution agreements, corrective action plans, and monetary settlements totaling $6,035,000.[3]

Recommendations

There is a continued need for regulated entities to improve compliance with the HIPAA Privacy, Security, and Breach Notification Rules (collectively, the HIPAA Rules). In particular, in its 2023 breach investigations, OCR identified the Security Rule standards[4] and implementation specifications[5] of risk analysis, risk management, information system activity review, audit controls, and person or entity authentication as key areas for improvement.

---

[1] This figure reflects the number of breaches affecting 500 or more individuals that occurred or ended in calendar year 2023. In total, OCR received 746 breach reports via the HIPAA Breach Web Portal in 2023, but some of these breaches did not occur in 2023 (*e.g.*, breach occurred in 2022, and was reported to OCR in 2023).

[2] This figure reflects the number of breaches affecting under 500 individuals that occurred or ended in calendar year 2023.

[3] The seven breach investigations resolved in 2023 through resolution agreements, corrective action plans, and monetary settlements were MedEvolve, Yakima Valley Memorial Hospital, iHealth Solutions, Doctors' Management Services, Lafourche Medical Group, Montefiore Medical Center, and Green Ridge Behavioral Health.

[4] *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".

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

As in previous years, hacking/IT incidents remained the largest category of breaches of unsecured PHI affecting 500 or more individuals that occurred in 2023, comprising 81% of such reported breaches. Hacking/IT incidents also affected the most individuals (108,725,761) whose PHI was involved in breaches of unsecured PHI affecting 500 or more individuals. The largest category of breaches of unsecured PHI affecting 500 or more individuals by location of PHI was network servers. For breaches of unsecured PHI affecting fewer than 500 individuals that occurred in 2023, the largest category by type of breach report was unauthorized access or disclosure, and the largest category by location of PHI was paper records.

Background

The HIPAA Privacy Rule, found at 45 C.F.R. Part 160 and Subparts A and E of Part 164, protects the privacy of PHI, and gives individuals certain rights with respect to PHI, while permitting regulated entities to engage in 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. Regulated entities may not use or disclose PHI except as permitted or required by the Privacy Rule.

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[6] under HIPAA to notify affected individuals, 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 2023.

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 Secretary has issued guidance that identifies certain encryption and destruction processes tested by the National Institute of Standards and Technology as technologies and methodologies for rendering PHI unusable, unreadable, or indecipherable to unauthorized persons.[7] Covered entities and business associates that encrypt or destroy PHI in accordance with the Secretary's guidance are not required to provide notifications in the event of a breach of such information because such information is not considered "unsecured."

[6] A covered entity is a health plan, a health care clearinghouse, or a health care provider that transmits any health information in electronic form in connection with a transaction for which HHS has adopted a standard (*e.g.,* health care claims and equivalent encounter information, enrollment and disenrollment in a health plan, health care payment and remittance advice).

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

HHS promulgated a final rule regarding Breach Notification for Unsecured Protected Health Information on January 25, 2013 (78 FR 5566) (the Breach Notification Rule). OCR is the office within HHS that is responsible for administering and enforcing the HIPAA Privacy, Security, and Breach Notification Rules.

Definition of Breach

Consistent with the definition of breach in section 13400(1)(A) of the HITECH Act, the Breach Notification Rule 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, an unauthorized acquisition, access, use, or disclosure of PHI (that does not fall into one of the enumerated exceptions discussed below) is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment. This risk assessment must address at least the following factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person(s) who used the PHI or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated.[8]

Section 13400(1)(B) of the HITECH Act provides several exceptions to the definition of "breach." These exceptions are set forth in the Breach Notification Rule 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 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.[9] These breach notification requirements for covered entities and business associates are set forth at 45 CFR §§ 164.404 – 164.410.

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

[9] 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 withoutunreasonable 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.[10]

- **Media Notice**

For breaches of unsecured PHI 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.[11]

- **Notice to the Secretary**

In addition to notifying affected individuals and the media (where appropriate), a covered entitymust notify the Secretary of breaches of unsecured PHI. If a breach of unsecured PHI involves 500 or more individuals, a covered entity must notify the Secretary at the same time the affected individuals are notified of the breach.[12] If a breach of unsecured PHI involves fewer than 500 individuals, covered entities may submit reports of such breaches on an annual basis. Reports of breaches of unsecured PHI 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.[13] Covered entities must

[10] *See* 45 CFR § 164.404.
[11] *See* 45 CFR § 164.406.
[12] *See* 45 CFR § 164.408(b).
[13] *See* 45 CFR § 164.408(c).

notify the Secretary by filling out and electronically submitting a breach report form on the HHS 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 mustnotify 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 calendardays 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) when a breach of unsecured PHI 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.[14]

Investigations

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

In some cases, an OCR investigation may determine that there is insufficient evidence to support a finding that a covered entity or business associate violated the HIPAA Rules. In such cases, OCR may send 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 the regulated entity's compliance through corrective action, which may include a resolution agreement.

Where corrective action is sought, OCR may obtain 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 typically pursues a resolution 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

[14] 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.

that, while OCR is prepared to assess a civil money penalty (CMP) with regard to identified 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 generally involve the payment of a monetary settlement 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 the investigated entities' noncompliance and deter future noncompliance with the HIPAA Rules, and when OCR announces those resolutions, the announcements serve as reminders to the wider regulated community of their own HIPAA compliance 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 OCR proposes a CMP, 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 section describes the types and numbers of breaches of unsecured PHI reported to OCR that occurred between January 1, 2023, and December 31, 2023, and describes actions taken by covered entities and business associates in response to these breaches.

This section also generally describes OCR investigations and enforcement actions with respect to the reported breaches of unsecured PHI. 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 2023*. OCR opens compliance reviews to investigate all reported breaches affecting 500 or more individuals and may open compliance reviews into reported breaches affecting fewer than 500 individuals. As discussed in greater detail below, in 2023, in addition to requiring covered entities and business associates to take corrective action in hundreds of cases, OCR resolved seven breach investigations with resolution agreements, corrective action plans, and monetary settlements totaling $6,035,000.

As shown in the table on the next page, the number of breaches of unsecured PHI reported to OCR continues to increase. Between 2019 and 2023, the number of reported breaches of unsecured PHI affecting fewer than 500 individuals increased by 9% and the number of reported breaches of unsecured PHI affecting 500 or more individuals rose by 79%.

Year	Under 500 Breaches Reported	500+ Breaches Reported	Percentage Change in Under 500 Breaches Reported	Percentage Change in 500+Breaches Reported
2023	68,315	732	7% increase	17% increase
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	-	-
2019 to 2023	9% increase	79% increase	-	-

Source: Current and previous Reports to Congress https://www.hhs.gov/ocr/about-us/reports/index.html

Breaches Involving 500 or More Individuals

Notification to the Secretary of breaches of unsecured PHI involving 500 or more individuals must occur contemporaneously with notice to affected individuals. OCR received 732 reports of such breaches that occurred in calendar year 2023,[15] which affected a total of approximately 113,173,613 individuals.[16]

[15] HHS receives some reports of breaches that 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 2021 into 2023 would be included in the 2023 figures).

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

Breaches in 2023 Affecting 500 or More Individuals[17]

For the 732 breaches of unsecured PHI affecting 500 or more individuals in 2023, OCR received:

(1) 461 breach reports (63% of total breach reports) from health care providers (affecting 43,048,365 individuals (38% of total affected individuals));

(2) 152 breach reports (21% of total breach reports) from business associates (affecting 55,519,648 individuals (49% of total affected individuals));

(3) 116 breach reports (16%) from health plans (affecting 14,600,391 individuals (13% of total affected individuals)); and

(4) 3 breach reports (<1% of total breach reports) from health care clearinghouses (affecting 5,209 individuals (<1% of total affected individuals)).

See Figures 1 and 2.

HHS Office for Civil Rights Reports of Breaches of Unsecured PHI Affecting 500 or more Individuals in 2023 by Percentage of Reports Received for each Entity Type

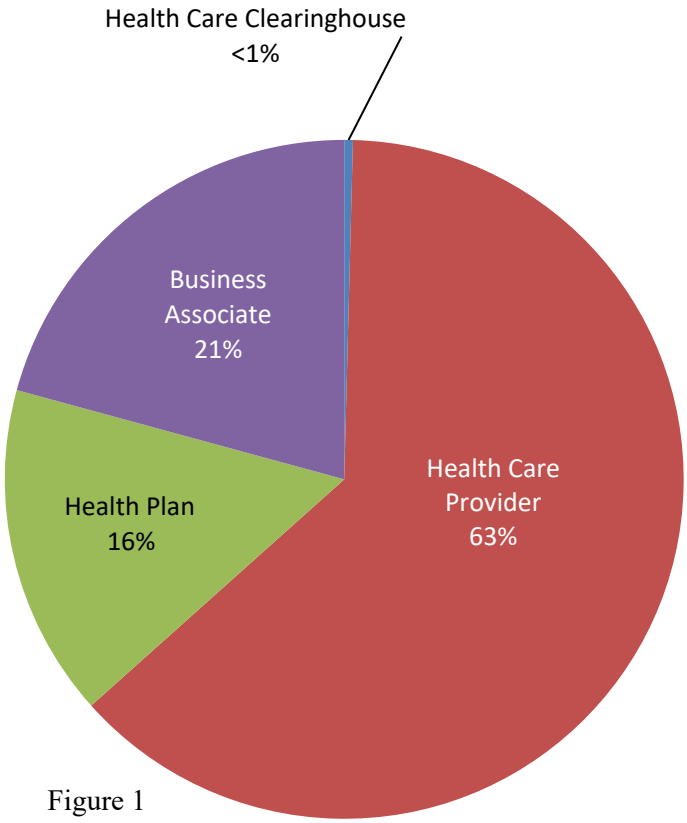

Figure 1

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

HHS Office for Civil Rights Reports of Breaches of Unsecured PHI Affecting 500 or more Individuals in 2023 by Percentage of Affected Individualsfor each Entity Type

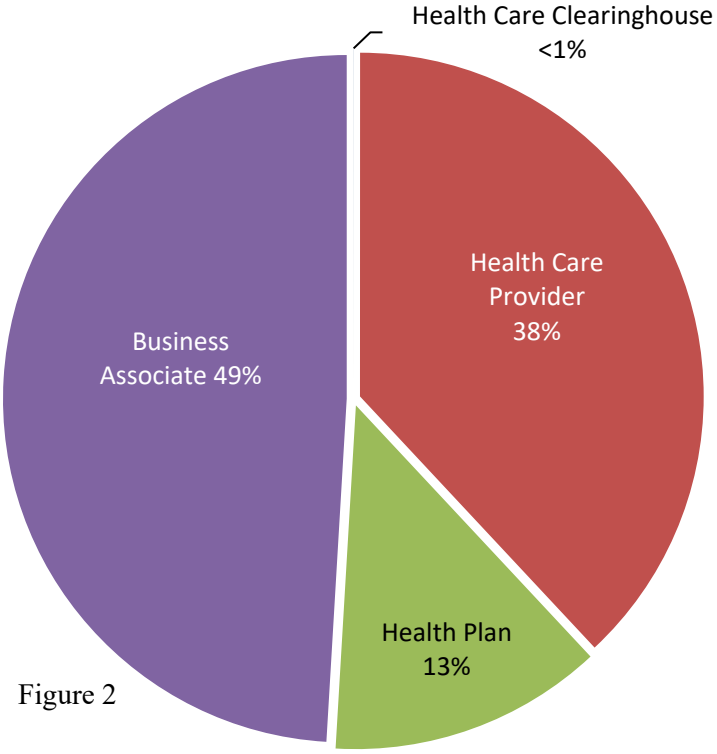

Figure 2

The 732 reports submitted to OCR for breaches of unsecured PHI affecting 500 or more individuals occurring in 2023 can be categorized by five general types or causes as follows (in order of frequency):[18]

(1) Hacking/IT incident involving electronic equipment or a network server (590 breach reports (81% of total breach reports) affecting 108,725,761 individuals (96% of total affected individuals));

(2) Unauthorized access or disclosure of records containing PHI (120 breach reports (16% of total breach reports) affecting 4,359,037 individuals (4% of total affected individuals));

(3) Theft of electronic equipment/portable devices or paper containing PHI (14 breach reports (2% of total breach reports) affecting 69,893 individuals (<1% of total affected individuals));

(4) Loss of electronic media or paper records containing PHI (4 breach reports (1% of total breach reports) affecting 16,247 individuals (<1% of total affected individuals)); and

(5) Improper disposal of PHI (4 breach reports (1% of total breach reports) affecting 2,675 individuals (<1% of total affected individuals)).

See Figures 3 and 4.

[18] Only one cause or type of breach can be selected by regulated entities in the breach report to HHS. Regulated entities select the type of breach using the definitions on the form in the HHS Breach Web Portal.

HHS Office for Civil Rights Reports of Breaches of Unsecured PHI Affecting 500 or more Individuals in 2023 by Percentage of Reports Received for each Type of Breach

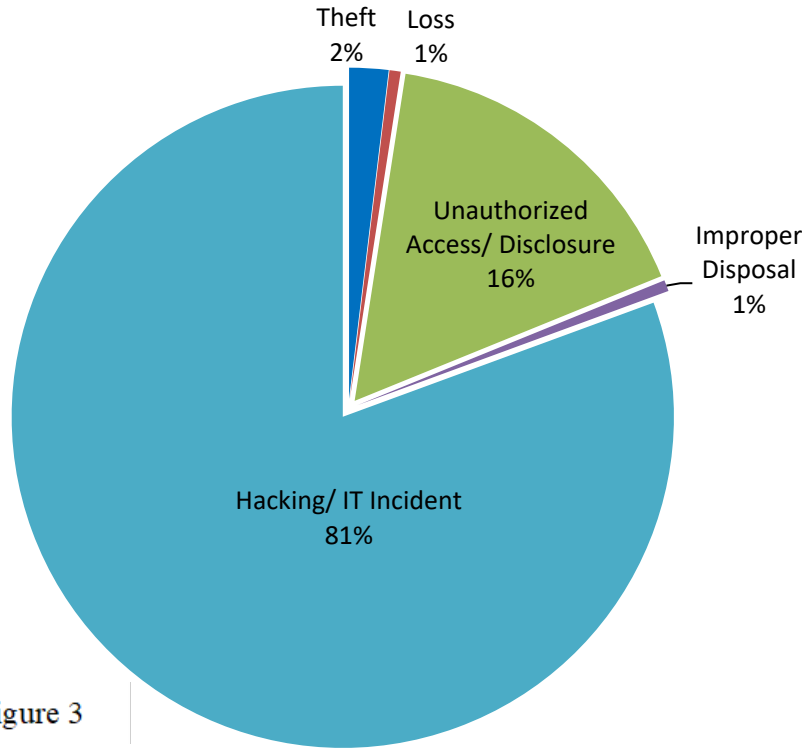

Figure 3

HHS Office for Civil Rights Reports of Breaches of Unsecured PHI Affecting 500 or more Individuals in 2023 by Percentage of Affected Individuals for each Type of Breach

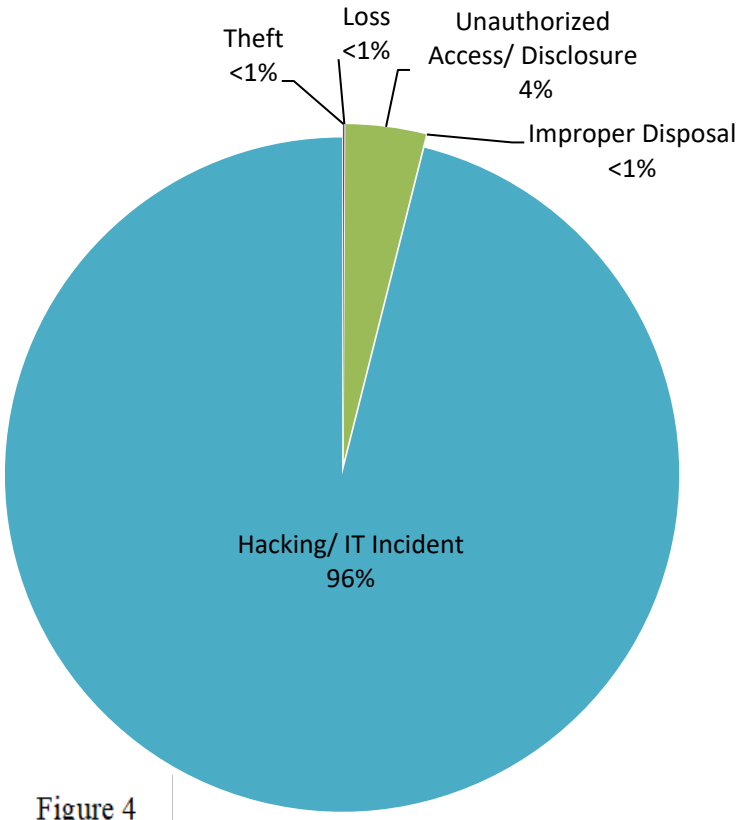

Figure 4

The 732 reports submitted to OCR for breaches of unsecured PHI occurring in 2023 described the following locations of the PHI (in order of frequency):[19]

(1) Network server (485 breach reports (66% of total breach reports) affecting 108,248,461 individuals (96% of total affected individuals));
(2) E-mail (120 breach reports (16% of total breach reports) affecting 1,851,605 individuals (2% of total affected individuals));
(3) Paper (44 breach reports (6% of total breach reports) affecting 236,478 individuals (<1% of total affected individuals));
(4) Electronic medical record (24 breach reports (3% of total breach reports) affecting 1,608,617 individuals (1% of total affected individuals));
(5) Desktop computer (40 breach reports (5% of total breach reports) affecting 1,071,311 individuals (1% of total affected individuals));
(6) Other portable electronic device (7 breach reports (1% of total breach reports) affecting 81,428 individuals (<1% of total affected individuals));
(7) Laptop computer (12 breach reports (2% of total breach reports) affecting 75,713 individuals (< 1% of total breach reports)); and
(8) Other (0 breach reports (0% of total breach reports) affecting 0 individuals (0% of total affected individuals)).[20]

See Figures 5 and 6.

HHS Office for Civil Rights Reports of Breaches of Unsecured PHI Affecting 500 or moreIndividuals in 2023 by Percentage of Reports Received for each Location of PHI

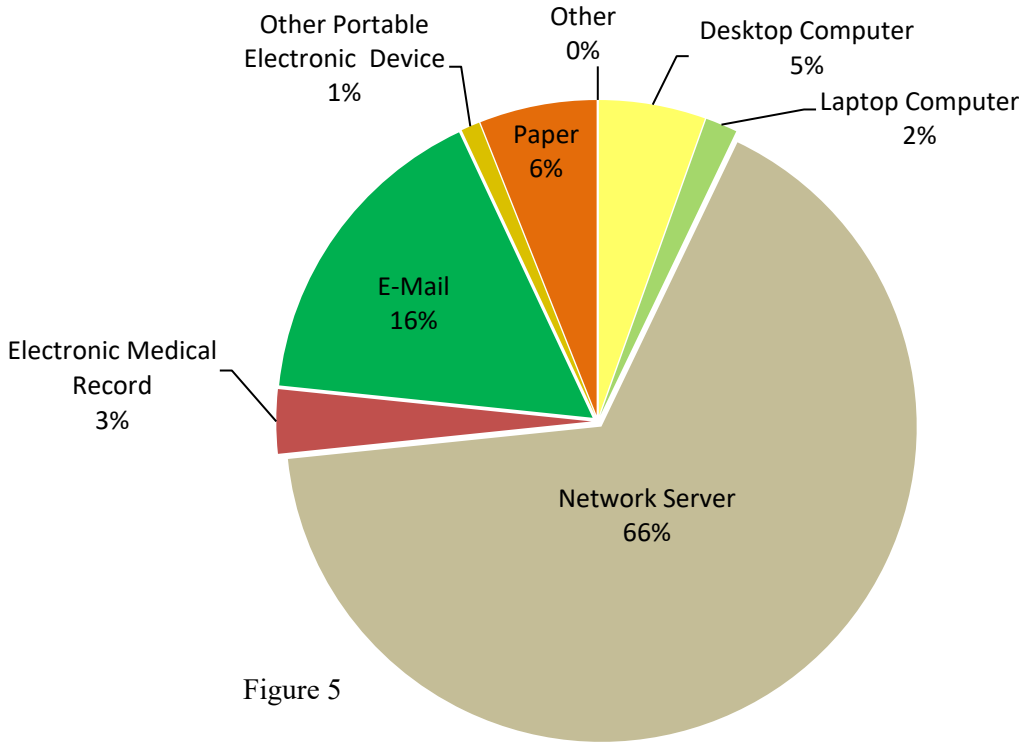

Figure 5

[19] A breach may occur in more than one location. The reporting entity selects the main location of the breach incompiling this data.
[20] "Other" is used when a regulated 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 regulated entity is not certain of the PHI's location when it was disclosed.

HHS Office for Civil Rights Reports of Breaches of Unsecured PHI Affecting 500 or More Individuals in 2023 by Percentage of Affected Individuals for each Location of PHI

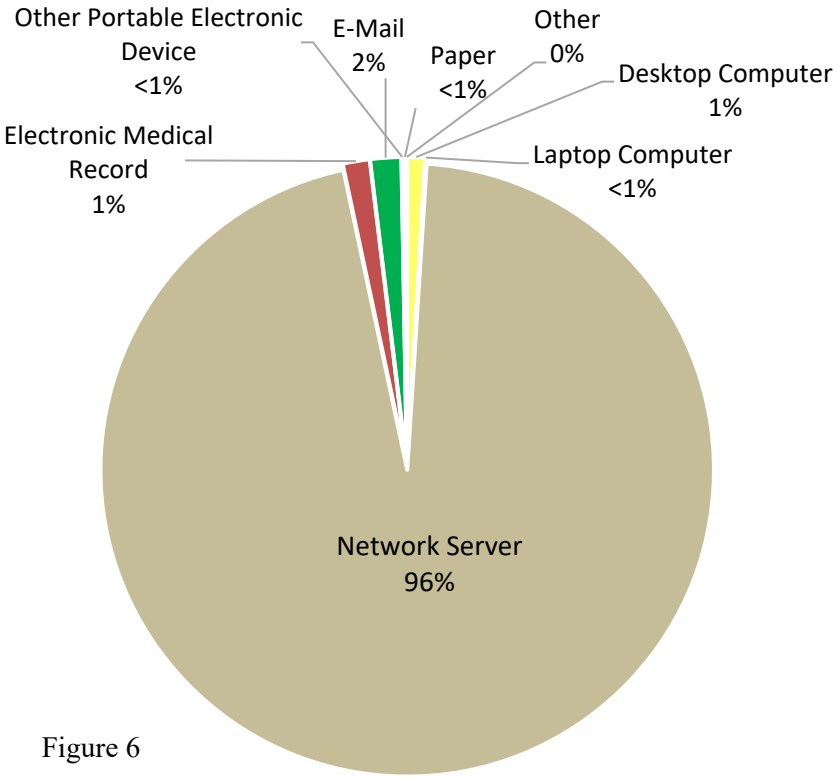

Figure 6

Largest breaches in 2023 for each reported breach type or cause

This section describes the largest breaches of unsecured PHI, by number of affected individuals, for each of the five reported general breach types or causes, followed by a short summary of scenarios reported for each type or cause.

Hacking/IT Incident of Electronic Equipment or Network Server: The largest reported breach of unsecured PHI in 2023 resulted from a hacking/IT incident in which hackers deployed malware that compromised the servers of a healthcare provider containing electronic PHI (ePHI). The breach incident affected approximately 11,270,000 individuals. Other hacking/IT incidents involved the use of ransomware, phishing, and the posting of PHI to public websites.

Unauthorized Access or Disclosure of PHI: The largest reported breach of unsecured PHI in 2023 involving the unauthorized access or disclosure of ePHI affected approximately 3,179,835 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 2023 resulted from a covered entity who improperly disposed of patient logs by throwing them away in a dumpster. This breach affected approximately 1,005 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 2023 resulted from the theft of a laptop when a medical office was burglarized. The theft affected approximately 34,016 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 a storage unit that was sold due to non-payment. The storage unit contained the PHI of 13,184 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 2023, 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 protectionof health information.

Breaches Involving Fewer than 500 Individuals

Notification to the Secretary of breaches of unsecured PHI involving fewer than 500 individuals must occur no later than 60 days after the end of the calendar year in which the breaches are discovered. For breaches discovered during 2023, notification to OCR was required no later than March 1, 2024. OCR received 68,315 reports of breaches involving fewer than 500 individuals that occurred in calendar year 2023, which affected a total of approximately 269,290 individuals.

Breaches involving fewer than 500 individuals for 2023

For the 68,315 reports of breaches of unsecured PHI affecting fewer than 500 individuals, OCR received:

(1) 62,939 breach reports (92% of total breach reports) from health care providers affecting 206,278 individuals (77% of total affected individuals);
(2) 3,957 breach reports (6% of total breach reports) from health plans affecting 34,234 individuals (13% of total affected individuals);
(3) 1,379 breach reports (2% of total breach reports) from business associates affecting 28,592 individuals (11% of total affected individuals); and
(4) 40 breach reports (<1% of total breach reports) from health care clearinghouses affecting 186 individuals (<1% of total affected individuals).

See Figures 7 and 8.

HHS Office for Civil Rights Reports of Breaches of Unsecured PHI Affecting Fewer Than 500 Individuals in 2023 by Percentage of Reports Received for each Entity Type

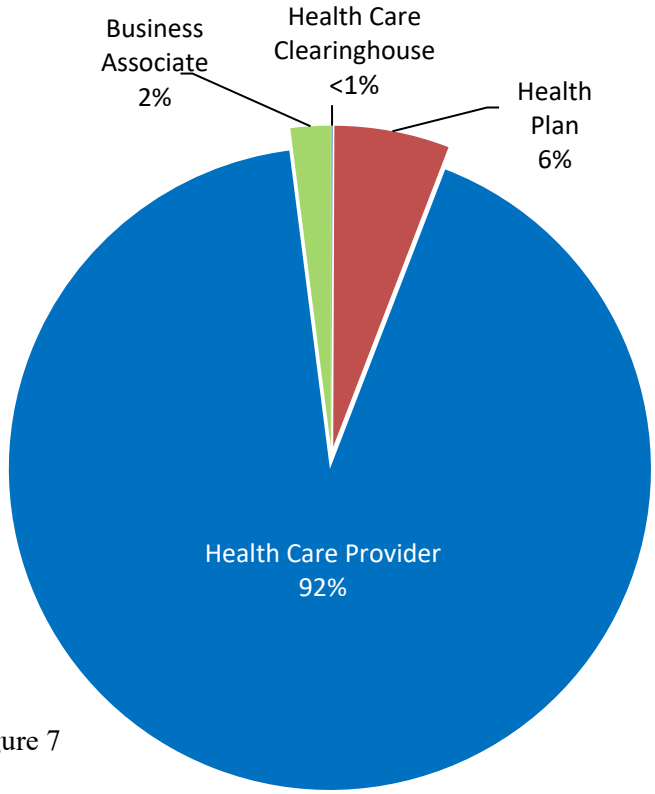

Figure 7

HHS Office for Civil Rights Reports of Breaches of Unsecured PHI Affecting Fewer Than 500 Individuals in 2023 by Percentage of Affected Individuals for each Entity Type

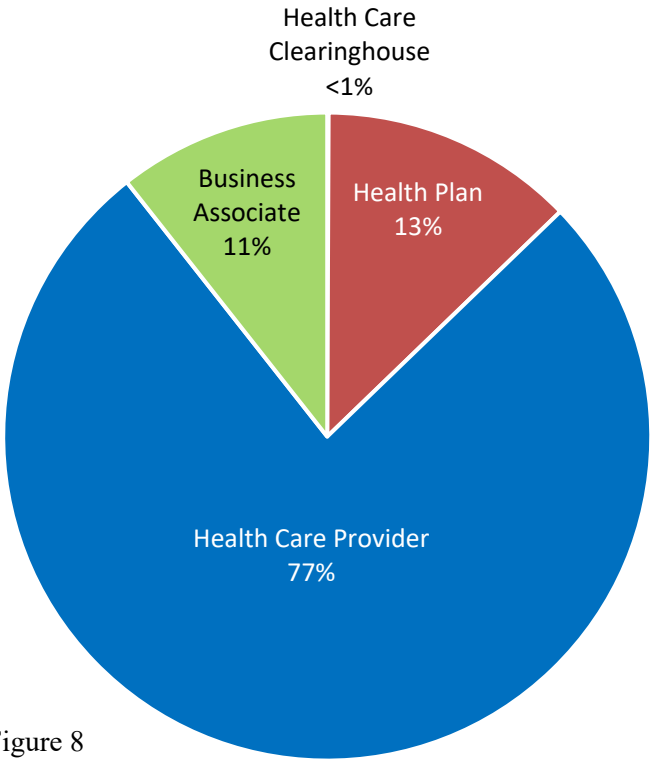

Figure 8

The 68,315 reports submitted to OCR for breaches of unsecured PHI affecting fewer than 500 individuals occurring in 2023 can be categorized by five general types or causes as follows (in order of frequency):[21]

(1) Unauthorized access or disclosure of records containing PHI (64,231 breach reports (94% of total breach reports) affecting 178,031individuals (66% of total affected individuals));
(2) Loss of electronic media or paper records containing PHI (2,414 reports (4% of total breach reports) affecting 10,186 individuals (4% of total affected individuals));
(3) Hacking/IT incident involving electronic equipment or a network server (753 reports (1% of total breach reports) affecting 61,021 individuals (23% of total affected individuals));
(4) Theft of electronic equipment/portable devices or paper containing PHI (714 reports (1% of total breach reports) affecting 15,742 individuals (6% of total affected individuals)); and
(5) Improper disposal of PHI (203 reports (<1% of total breach reports) affecting 4,310 individuals (2% of total affected individuals)).

See Figures 9 and 10.

HHS Office for Civil Rights Reports of Breaches of Unsecured PHI Affecting Fewer Than 500 Individuals in 2023 by Percentage of Reports Received for each Type of Breach

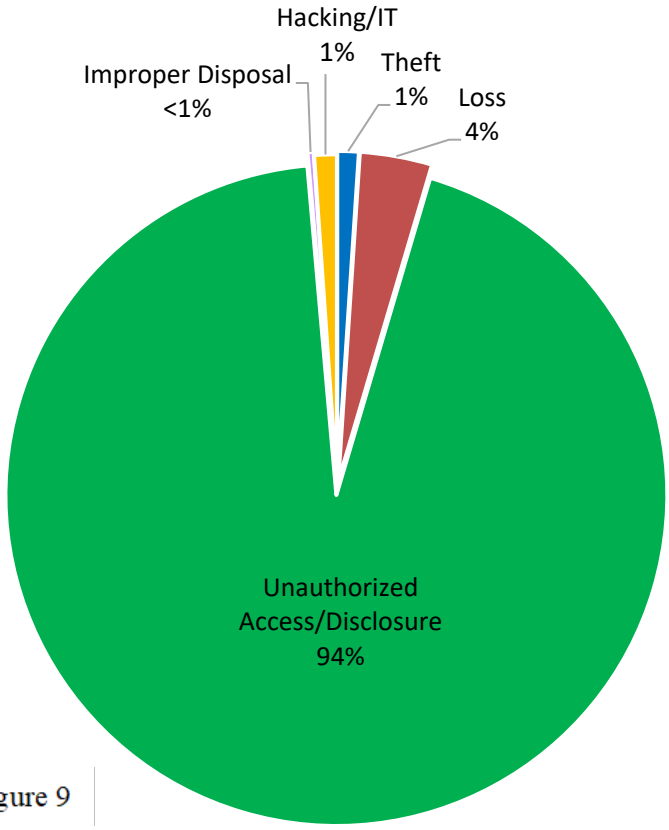

Figure 9

[21] 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 Reports of Breaches of Unsecured PHI Affecting Fewer Than 500 Individuals in 2023 by Percentage of Affected Individuals for each Type of Breach

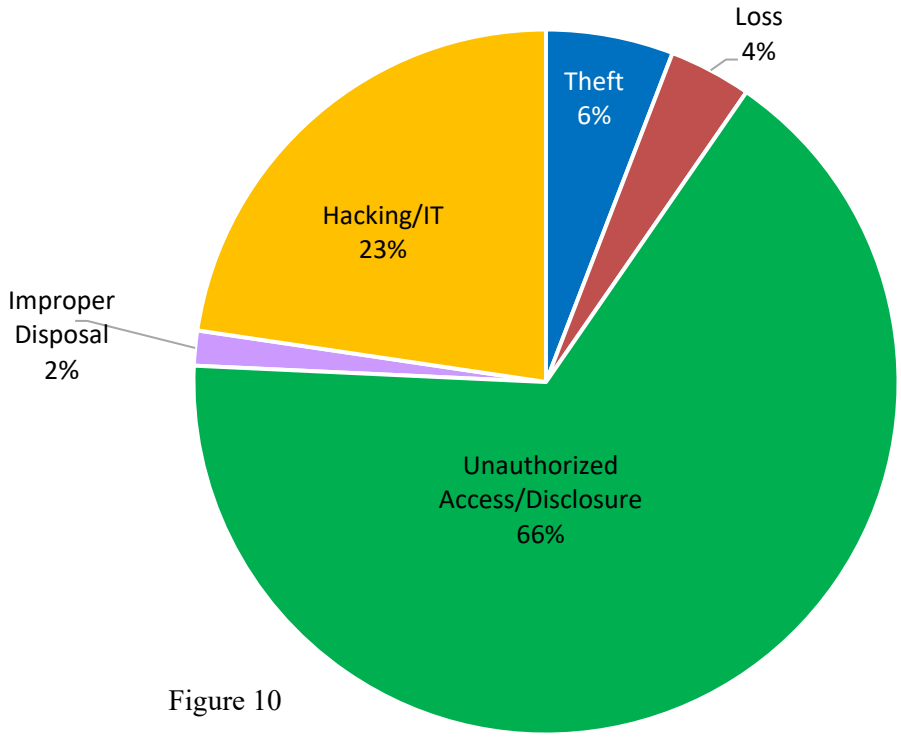

Figure 10

The 68,315 reports submitted to OCR for breaches of unsecured PHI affecting fewer than 500 individuals described the following locations of the PHI (in order of frequency):[22]

(1) Paper (41,402 reports (61% of total breach reports) affecting 87,478 individuals (32% of total affected individuals));
(2) Electronic medical record (EMR) (13,255 reports (19% of total breach reports) affecting 37,198 individuals(14% of total affected individuals));
(3) Other (7,214 reports (11% of total breach reports) affecting 35,529 individuals (13% of total affected individuals));[23]
(4) E-mail (3,845 reports (6% of total breach reports) affecting 53,282 individuals (20% of total affected individuals));
(5) Other portable electronic device (915 reports (1% of total breach reports) affecting 4,713 individuals (2% of total affected individuals));
(6) Desktop computer (896 reports (1% of total breach reports) affecting 6,838 individuals (3% of total affected individuals));
(7) Network server (576 reports (1% of total breach reports) affecting 37,858 individuals (14% of total affected individuals)); and
(8) Laptop computer (212 reports (< 1% of total breach reports) affecting 6,394 individuals (2% of total affected individuals)).

See Figures 11 and 12.

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

HHS Office for Civil Rights Reports of Breaches of Unsecured PHI Affecting Fewer Than 500 Individuals in 2023 by Percentage of Reports Received for each Location of PHI

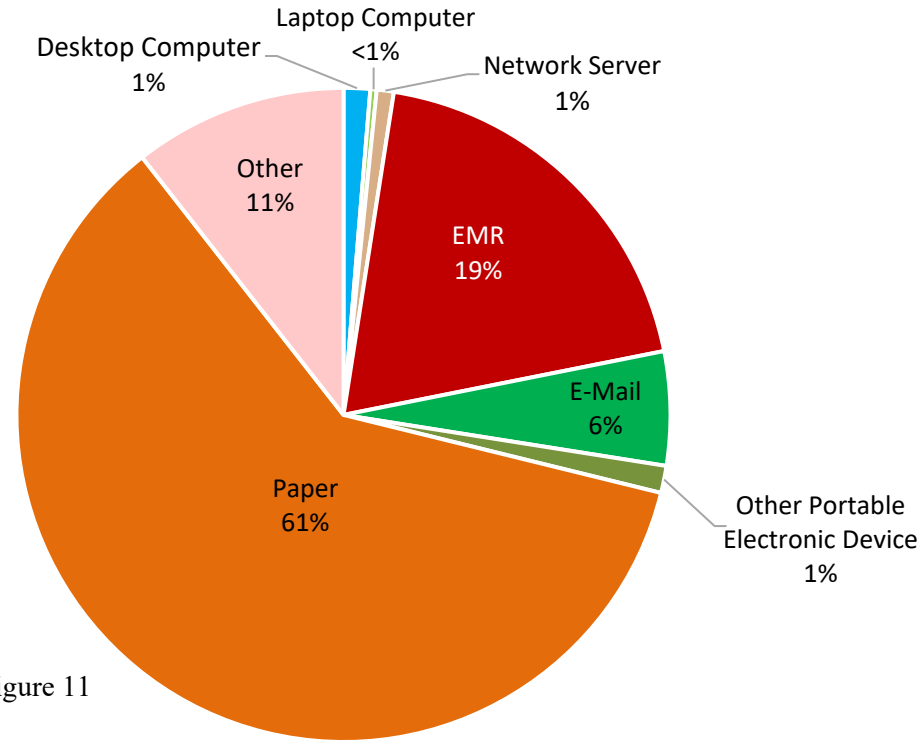

Figure 11

HHS Office for Civil Rights Reports of Breaches of Unsecured PHI Affecting Fewer Than 500 Individuals in 2023 by Percentage of Affected Individuals for each Location of PHI

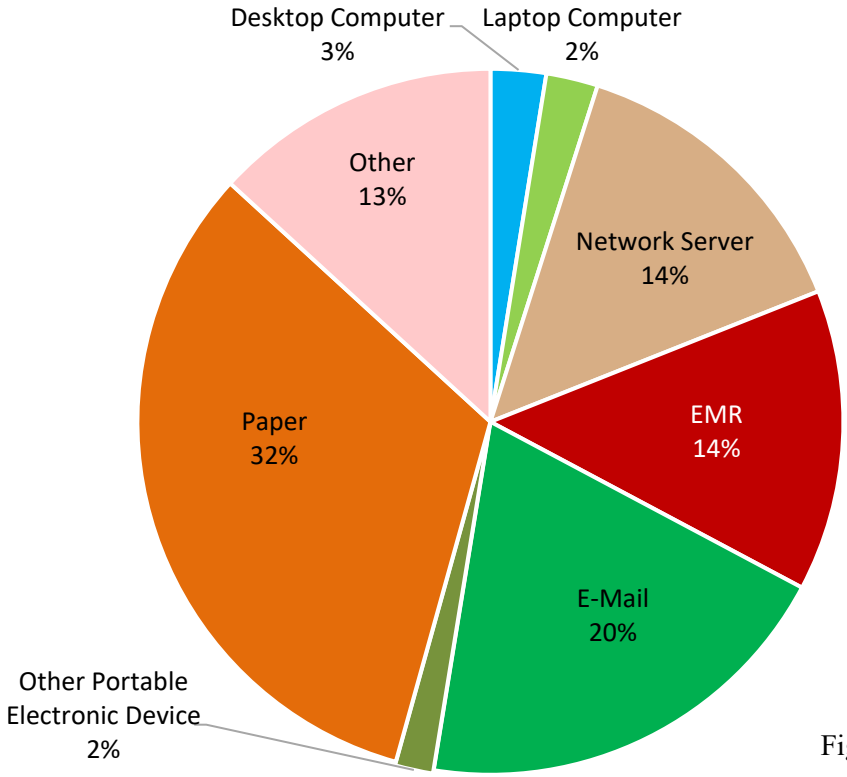

Figure 12

Details on breaches involving fewer than 500 individuals for 2023

As in previous years, breach incidents reported for 2023 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 2023 were due to employees who impermissibly accessed the medical records of co-workers, family, friends, and other individuals. In response to these incidents, covered entities commonly reported taking remedial actions such as fixing "glitches" in software that incorrectly compiled lists of patient names and contact information, revising policies and procedures,training or retraining employees who handle PHI, and sanctioning employees.

OCR completed nine breach investigations involving fewer than 500 individuals in 2023.

Cases Investigated and Action Taken

OCR opened investigations into all 732 reported breaches affecting 500 or more individuals that occurred in 2023. OCR also opened 9 investigations into breaches affecting fewer than 500 individuals. OCR completed 724 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 2023 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 2023*.

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 2023 as areas needing improvement:

- Security Management Process Standard.[24] 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 as identified by OCR's investigations and compliance reviews conducted in 2023 include:
    - Risk Analysis.[25] The Security Rule requires regulated entities to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the regulated entity. Security Rule investigations in 2023 found

[24] 45 C.F.R. §164.308(a)(1).
[25] 45 C.F.R. §164.308(a)(1)(ii)(A).

numerous instances where regulated entities' risk analyses lacked a comprehensive identification and assessment of the potential risks and vulnerabilities to ePHI in their environments. Specifically, risk analyses, if conducted at all, were often based on incomplete knowledge of where ePHI is created, received, maintained, or transmitted, resulting in incomplete assessments of risks and vulnerabilities that were deficient in scope. Failures to conduct an accurate and thorough risk analysis allow risks and vulnerabilities to go undetected and thus unmitigated leaving regulated entities vulnerable to breaches of unsecured ePHI as cybersecurity attacks are increasing.

- Risk Management.[26] 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 mitigate risks and vulnerabilities as part of a risk management process leaves regulated entities vulnerable to breaches of unsecured ePHI as cybersecurity attacks are increasing.

- Information System Activity Review.[27] The Security Rule requires regulated entities to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. OCR's investigations in 2023 continued to find instances of deficient or non-existent information system activity review processes. Examples of deficient processes include a total lack of reviews of any activity of the regulated entity's information systems as well as reviews that were ad hoc, reactive, or deficient in scope. A regulated entity's irregular or insufficient review of its information systems leaves access to ePHI unmonitored. A successful information 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.[28] 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, such as logs recording user and system activity, can help detect suspicious activity that may indicate information systems have been compromised. Further, reviews of such logs can help identify malicious activity that previously occurred which can inform incident response and mitigation activities. Maintaining robust audit controls can be important for regulated entities to understand how attackers gained access to information systems and to help identify the scope of malicious actions. OCR's investigations continued to find regulated entities that either do not have audit control mechanisms in

[26] 45 C.F.R. §164.308(a)(1)(ii)(B).
[27] 45 C.F.R. §164.308(a)(1)(ii)(D).
[28] 45 C.F.R. §164.312(b).

place or have implemented audit control mechanisms for only a narrow subset of its information systems that contain or use ePHI. Additionally, OCR's investigations have found regulated entities implementing deficient audit control procedures, such as not maintaining logs for a sufficient period of time such that information concerning malicious activity is unavailable or logs that do not capture relevant information (*e.g.*, level of detail is not sufficient). 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 and thus contribute to adverse impacts of cybersecurity attacks.

- Person or Entity Authentication.[29] The Security Rule requires regulated entities to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed. Compromised credentials continue to be one of the leading ways by which attackers gain unauthorized access to a regulated entity's network and information systems. In 2023, OCR's investigations found multiple instances of ineffective authentication procedures including allowing weak passwords and the use of weak authentication solutions in higher risk use cases (*e.g.*, remote access requiring only single-factor authentication). Many of OCR's investigations revealed that many regulated entities only implement multi-factor authentication after a breach has occurred. In June 2023, OCR published a cybersecurity newsletter strongly advocating that regulated entities consider implementing multi-factor authentication solutions as part of the cybersecurity strategy and as a means to meet HIPAA's authentication requirement. Strong authentication, such as multi-factor 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 81% of the reports received and 96% of the individuals affected in 2023. Health care providers experienced the majority of these (63%), which affected over 43 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 2023, unauthorized access or disclosure was the largest category of type of breach reported (94%), and paper records was the largest by location (61%).

The breach notification requirements increase transparency of breaches both with the public at-large and within the regulated industry, as well as promote 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

[29] 45 C.F.R. §164.312(d).

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 enforcement and compliance 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 2023, OCR resolved seven breach investigations with resolution agreements/corrective action plans and collected settlements totaling over $6 million.[30]

[30] The seven cases were MedEvolve, iHealth Solutions, Yakima Valley Memorial Hospital, Doctors' Management Services, Green Ridge Behavioral Health, Lafourche Medical Group, and Montefiore Medical Center.

APPENDIX

Resolution Agreements[31] in 2023

Resolution Agreement with MedEvolve

MedEvolve paid $350,000 and agreed to take corrective actions to settle potential violations of the HIPAA Privacy and Security Rules. MedEvolve is a business associate that provides practice management, revenue cycle management, and practice analytics software services to health care entities.

OCR began investigating MedEvolve after it filed a breach report in July 2018, stating that due to a misconfiguration of its server, the PHI of 230,572 individuals was left unsecure and accessible on the Internet. The potential HIPAA violations in this case included the impermissible disclosure of PHI of 230,572 individuals; a failure to conduct an accurate and thorough risk analysis to determine risk and vulnerabilities to its information systems; and a failure to enter into a business associate agreement with a subcontractor.

In addition to the monetary settlement, MedEvolve agreed to:

- Conduct an accurate and thorough risk analysis;
- Develop a 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 Privacy and Security 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 March 2023. The resolution agreement is available at the following link:
www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/medevolve-ra-cap/index.html

Resolution Agreement with iHealth Solutions

iHealth Solutions (iHealth) paid $75,000 and agreed to take corrective actions to settle potential violations of the HIPAA Privacy and Security Rules. iHealth is a business associate based in Kentucky that provides medical coding, billing, and information technology services to health care providers.

OCR began investigating iHealth after it filed a breach report in August 2017, stating that the PHI of 267 individuals was accessible over the Internet due to an unsecured server. OCR's

[31] 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 2023.

investigation determined that the potential HIPAA violations in this case included a failure to conduct an accurate and thorough risk analysis to determine risk and vulnerabilities to its information systems and a failure to develop a risk management plan.

In addition to the monetary settlement, iHealth agreed to:

- Conduct an accurate and thorough risk analysis;
- Develop a risk management plan to address and mitigate security risks and vulnerabilities found in the risk analysis;
- Implement a process for evaluating environmental and operational changes;
- Develop, maintain, and revise, as necessary, its written policies and procedures to comply with the HIPAA Privacy and Security Rules; and
- Distribute policies and procedures to workforce members.

This settlement occurred in April 2023. The resolution agreement is available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/ihealth-ra-cap/index.html

Resolution Agreement with Yakima Valley Memorial Hospital

Yakima Valley Memorial Hospital (Yakima) paid $240,000 and agreed to take corrective actions to settle a potential violation of the HIPAA Security Rule. Yakima is a community hospital located in central Washington.

OCR began investigating Yakima in May 2018 after it filed a breach report stating that an employee impermissibly accessed the PHI of 415 individuals. OCR's investigation found a potential violation of the HIPAA Security Rule's requirement to implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the Security Rule.

In addition to the monetary settlement, Yakima agreed to:

- Conduct an accurate and thorough risk analysis;
- Develop a 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;
- Train workforce members on the policies and procedures for the privacy and security of PHI; and
- Provide OCR with an accounting of all business associates and copies of all business associate agreements.

This settlement occurred in May 2023. The resolution agreement is available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/yakima-ra-cap/index.html

Resolution Agreement with Doctors' Management Services

Doctors' Management Services (DMS) paid $100,000 and agreed to take corrective actions to settle potential violations of the HIPAA Privacy and Security Rules. DMS is a medical management company based in Massachusetts that provides billing and payor credentialling to several covered entities.

In April 2019, OCR initiated an investigation after receiving a breach report from DMS stating that it experienced a ransomware attack that compromised the PHI of 206,695 individuals. OCR's investigation found that the potential violations of the HIPAA Privacy and Security Rules included the impermissible disclosure of the PHI of 206,695 individuals; a failure to conduct an accurate and thorough risk analysis that assessed technical, physical, and environmental risks and vulnerabilities associated with handling ePHI; a failure to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports; and a failure to implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the Security Rule.

In addition to the monetary settlement, DMS agreed to:

- Review and update its risk analysis;
- Update its risk management plan to address and mitigate security risks and vulnerabilities found in the updated risk analysis;
- Develop, maintain, and revise, as necessary, its written policies and procedures to comply with the HIPAA Security Rule;
- 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 September 2023. The resolution agreement is available at the following link:
www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/dms-ra-cap/index.html

Resolution Agreement with Green Ridge Behavioral Health

Green Ridge Behavioral Health (GRBH) paid $40,000 and agreed to take corrective actions to settle potential violations of the HIPAA Privacy and Security Rules. GRBH is multidisciplinary group practice that provides comprehensive outpatient mental health services in Washington, D.C.

In December 2019, OCR initiated an investigation after receiving a breach report from GRBH stating that it experienced a ransomware attack that compromised the PHI of approximately 14,000 individuals. OCR's investigation found that the potential violations of the HIPAA Privacy and Security Rules included the failure to conduct an accurate and thorough risk analysis of the potential risks and vulnerabilities to the confidentiality, integrity and availability of its ePHI; the failure to implement security measures sufficient to reduce risks and vulnerabilities to

ePHI to a reasonable and appropriate level; the failure to implement policies and procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports; and a failure to not use or disclose protected health information except as permitted by the Privacy Rule.

In addition to the monetary settlement, GRBH agreed to:

- Conduct an accurate and thorough risk analysis;
- Develop a risk management plan to address and mitigate security risks and vulnerabilities found in the risk analysis;
- Review, and as necessary, develop or revise certain written policies and procedures to comply with the HIPAA Privacy and Security Rules;
- Distribute these policies and procedures to workforce members;
- Train workforce members on the policies and procedures for the privacy and security of PHI; and
- Review all relationships with vendors and third-party service providers to identify business associates and provide HHS with an accounting of GRBH's business associates and provide copies of the business associate agreements that GRBH maintains with each business associate.

This settlement occurred in October 2023. The resolution agreement is available at the following link:
www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/green-ridge-behavioral-health-ra-cap/index.html

Resolution Agreement with Lafourche Medical Group

Lafourche Medical Group (LMG) paid $480,000 and agreed to take corrective actions to settle potential violations of the HIPAA Security Rule. LMG is a group practice providing medical services in Louisiana.

In May 2021, OCR received a breach report filed by LMG stating that one of its owners was the subject of an email phishing attack. LMG was unable to determine the exact number of individuals affected so, in its mitigation efforts, it provided breach notice to all of its 34,862 patients. OCR's investigation found that the potential violations of the HIPAA Security Rule included a failure to conduct an accurate and thorough risk analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its ePHI; and a failure to implement procedures to regularly review records of information system activity.

In addition to the monetary settlement, LMG agreed to:

- Conduct an accurate and thorough risk analysis;
- Develop a 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 Privacy and Security Rules;
- Distribute policies and procedures to workforce members; and
- Train workforce members on its policies and procedures for the privacy and security of PHI.

This settlement occurred in November 2023. The resolution agreement is available at the following link:
www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/lafourche-medical-group/index.html

Resolution Agreement with Montefiore Medical Center

Montefiore Medical Center (MMC) paid $4,750,000 and agreed to take corrective actions to settle potential violations of the HIPAA Security Rule. MMC is a not-for-profit academic medical center located in the Bronx borough of New York.

In July 2015, OCR received a breach report from MMC alleging that one of its employees inappropriately accessed the PHI of 12,517 individuals and sold this information to an identity theft ring. OCR's investigation found that the potential violations of the HIPAA Security Rule included a failure to conduct an accurate and thorough risk analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its ePHI; a failure to implement procedures to regularly review records of information system activity; and a failure to implement hardware, software, and/or procedural mechanisms that record and examine activity in all information systems that contain ePHI.

In addition to the monetary settlement, MMC agreed to:

- Conduct an accurate and thorough risk analysis;
- Develop a risk management plan to address and mitigate security risks and vulnerabilities found in the risk analysis;
- Implement audit controls using hardware, software, or procedural mechanisms that record and examine activity in all information systems that contain or use PHI;
- Review, and to the extent necessary, revise its written policies and procedures to comply with the HIPAA Privacy and Security 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 November 2023. The resolution agreement is available at the following link:
www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/montiefore/index.html