Annual Report to Congress on Breaches of Unsecured Protected Health Information

For Calendar Year 2024

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 2024 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 663 notifications[1] of breaches of unsecured PHI affecting 500 or more individuals that occurred during 2024, representing a decrease of 9% from the number of reports received in calendar year 2023. These reported breaches affected a total of approximately 242,908,056 individuals. The most reported category of breaches was hacking, and the largest breach of this type involved approximately 192,000,000 individuals. OCR also received 74,299 reports[2] of breaches affecting fewer than 500 individuals, with unauthorized access or disclosure as the most frequent type of breach reported. These smaller breaches affected a total of 340,618 individuals.

OCR initiated investigations into all the reported breaches of unsecured PHI affecting 500 or more individuals, as well as two reported breaches affecting fewer than 500 individuals. OCR resolved 785 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. OCR resolved 12 breach investigations with resolution agreements, corrective action plans, and monetary settlements, or civil money penalties totaling $7,813,831.

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 its 2024 breach investigations, OCR identified the Security Rule standards[3] and implementation specifications[4] of risk analysis, risk management, information system activity review, audit controls, and person or entity authentication as key areas for improvement.

As in previous years, hacking/IT incidents remained the largest category of breaches of unsecured PHI affecting 500 or more individuals that occurred in 2024, comprising 81% of such reported breaches. Hacking/IT incidents also affected the largest number of individuals (241,582,022)

[1] This figure reflects the number of breaches affecting 500 or more individuals that occurred or ended in calendar year 2024. In total, OCR received 742 breach reports via the HIPAA Breach Web Portal in 2024, but some of these breaches did not occur in 2024 (*e.g.*, breach occurred in 2023 and was reported to OCR in 2024).
[2] This figure reflects the number of breaches affecting under 500 individuals that occurred or ended in calendar year 2024.
[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."

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 2024, 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 CFR 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[5] 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[6] 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 2024.

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

[5] 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). 45 CFR 160.103 definition of "covered entity."

[6] Generally, a business associate is a person, other than a workforce member, that performs certain functions or activities for or on behalf of a covered entity, or that provides certain services to a covered entity involving the disclosure of PHI to the person. *See* 45 CFR 160.103 definition of "business associate."

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."

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 CFR 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 CFR 164.402. Section 164.402 excludes as a breach: (1) any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or business associate, if made in good faith and within the scope of authority, and if it does not result in further impermissible use or disclosure; (2) any inadvertent disclosure of PHI by a person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received is not further impermissibly used or disclosed; and (3) a disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain the information.

[7] https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html.
[8] *See* 45 CFR 164.402 (definition of a "breach").

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.

- **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.[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

[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.

[10] *See* 45 CFR 164.404.

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 entity must 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 maysubmit 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 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 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) 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

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

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 most 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 warrant 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 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, 2024, and December 31, 2024, 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 2024.* 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 2024, in addition to requiring covered entities and business associates to take corrective action in hundreds of cases, OCR resolved 12 breach investigations with resolution agreements, corrective action plans, and monetary settlements totaling $7,813,831.

As shown in the table below, the number of breaches of unsecured PHI reported to OCR continues to increase. Between 2020 and 2024, the number of reported breaches of unsecured PHI affecting fewer than 500 individuals increased by 12% and the number of reported breaches of unsecured PHI affecting 500 or more individuals rose by 1%.

Year	Under 500 Breaches Reported	500+ Breaches Reported	Percentage Change in Under 500 Breaches Reported	Percentage Change in 500+ Breaches Reported
2024	74,299	663	9% increase	9% decrease
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
2020 to 2024	12% increase	1% increase	-	-

Source: Current and previous Reports to Congress

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 663 reports of such breaches that occurred in calendar year 2024,[15] which affected a total of approximately 242,908,056 individuals.[16]

Breaches in 2024 Affecting 500 or More Individuals[17]

For the 663 breaches of unsecured PHI affecting 500 or more individuals in 2024, OCR received:

(1) 505 breach reports (76%) of total breach reports from health care providers (affecting 34,456,670 individuals (14% of total affected individuals));
(2) 106 breach reports (16%) of total breach reports from business associates (affecting 206,921,071individuals (85% of total affected individuals));
(3) 50 breach reports (8%) of total breach reports from health plans (affecting 1,303,493 individuals (1% of total affected individuals)); and
(4) 2 breach reports (<1%) of total breach reports from health care clearinghouses (affecting 226,822 individuals (<1% of total affected individuals)).

See Figures 1 and 2.

[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 2022 into 2024 would be included in the 2024 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.
[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 2024 by Percentage of Reports Received for each Entity Type

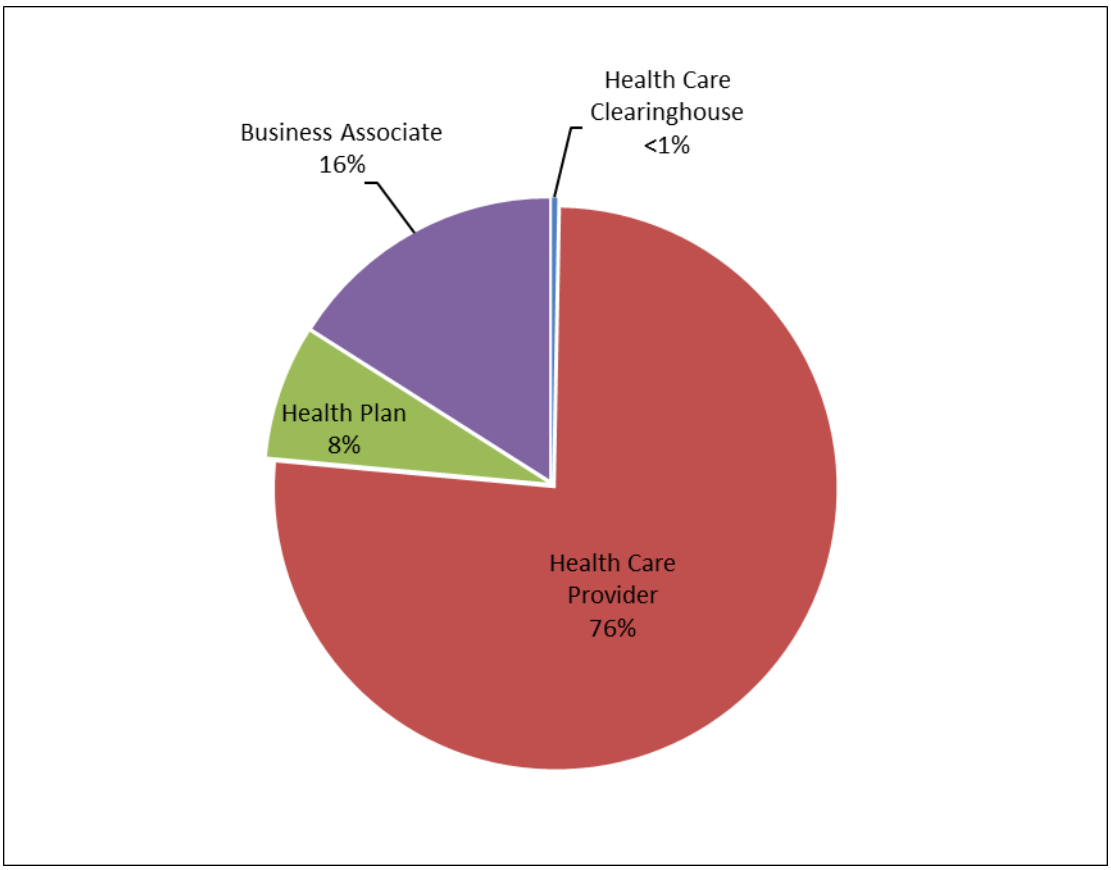

Figure 1

HHS Office for Civil Rights
Reports of Breaches of Unsecured PHI Affecting 500 or More Individuals in 2024 by Percentage of Affected Individuals for each Entity Type

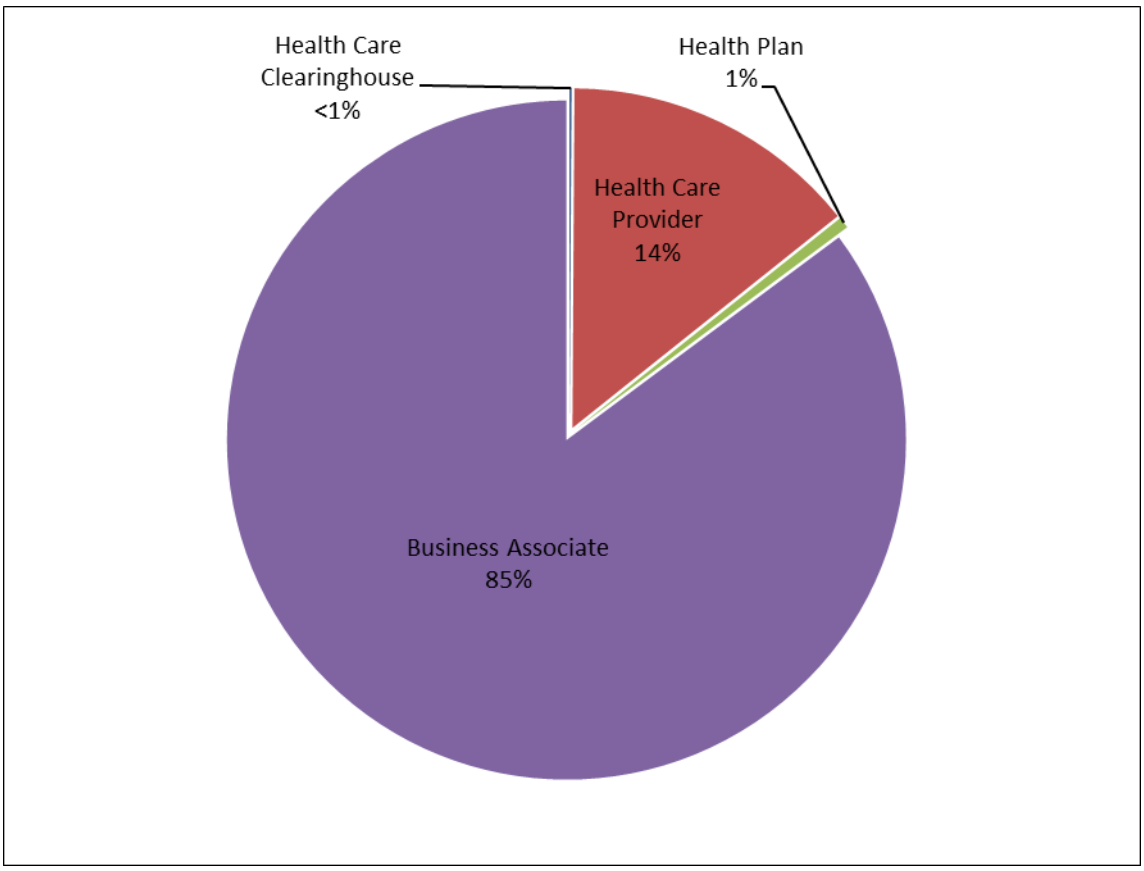

Figure 2

The 663 reports submitted to OCR for breaches of unsecured PHI affecting 500 or more individuals occurring in 2024 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 (534 breach reports (81% of total breach reports) affecting 241,582,022 individuals (99% of total affected individuals));
(2) Unauthorized access or disclosure of records containing PHI (108 breach reports (16% of total breach reports) affecting 1,256,501 individuals (1% of total affected individuals));
(3) Theft of electronic equipment/portable devices or paper containing PHI (16 breach reports (2% of total breach reports) affecting 54,500 individuals (<1% of total affected individuals));

[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.

(4) Improper disposal of PHI (3 breach reports <1% of total breach reports) affecting 9,809 individuals (<1% of total affected individuals)); and
(5) Loss of electronic media or paper records containing PHI (2 breach reports (<1% of total breach reports) affecting 5,224 individuals (<1% of total affected individuals)).

See Figures 3 and 4.

HHS Office for Civil Rights
Reports of Breaches of Unsecured PHI Affecting 500 or More Individuals in 2024 by Percentage of Reports Received for each Type of Breach

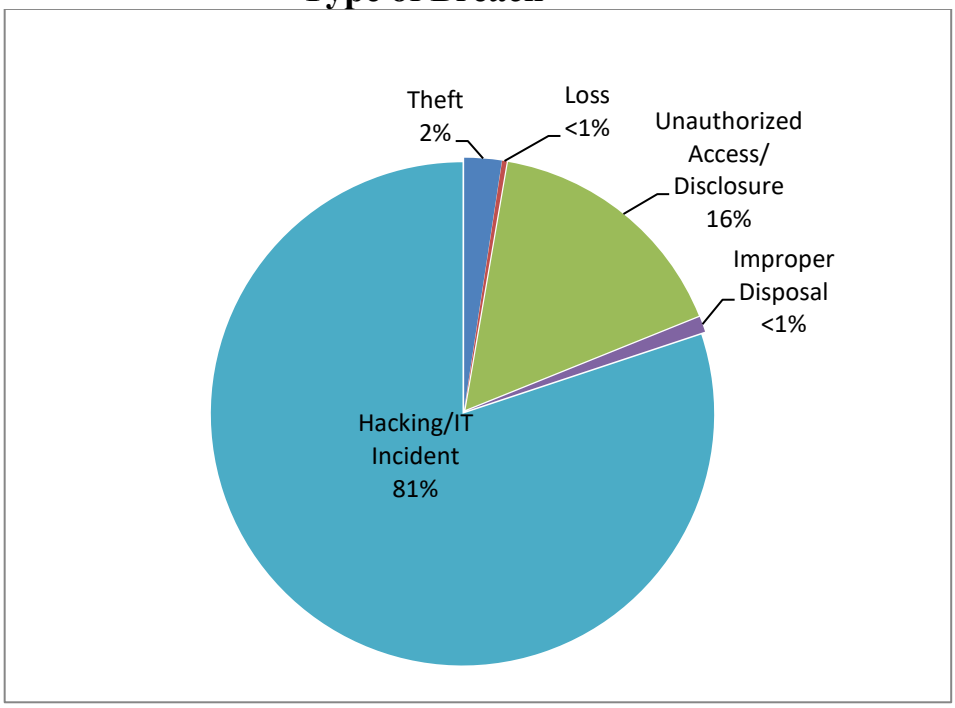

Figure 3

HHS Office for Civil Rights
Reports of Breaches of Unsecured PHI Affecting 500 or More Individuals in 2024 by Percentage of Affected Individuals for each Type of Breach

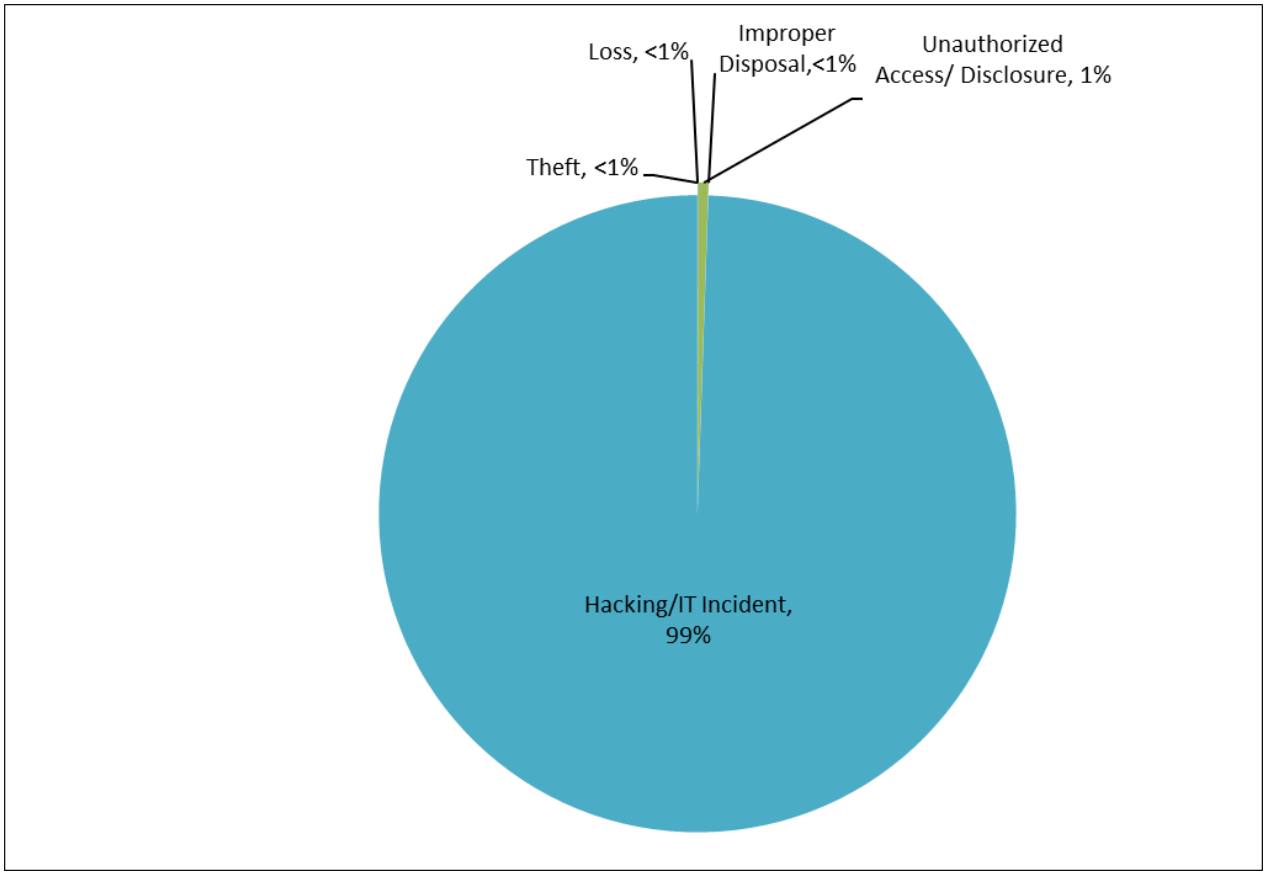

Figure 4

The 663 reports submitted to OCR for breaches of unsecured PHI occurring in 2024 described the following locations of the PHI (in order of frequency):[19]

(1) Network server (418 breach reports (63% of total breach reports) affecting 238,484,036 individuals (98% of total affected individuals));
(2) E-mail (164 breach reports (25% of total breach reports) affecting 3,974,177 individuals (2% of total affected individuals));
(3) Paper (34 breach reports (5% of total breach reports) affecting 117,047 individuals (<1% of total affected individuals));
(4) Electronic medical record (20 breach reports (3% of total breach reports) affecting 184,532 individuals (<1% of total affected individuals));
(5) Laptop computer (9 breach reports (1% of total breach reports) affecting 76,431 individuals (<1% of total affected individuals))

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

(6) Other (9 breach reports (1% of total breach reports) affecting 40,563 individuals <1% of total affected individuals));
(7) Other portable electronic device (7 breach reports (1% of total breach reports) affecting 28,207 individuals (< 1% of total breach reports)); and
(8) Desktop computer (2 breach reports (<1% of total breach reports) affecting 3,063 individuals (<1% of total affected individuals)).[20]

See Figures 5 and 6.

[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 2024 by Percentage of Reports Received for each Location of PHI

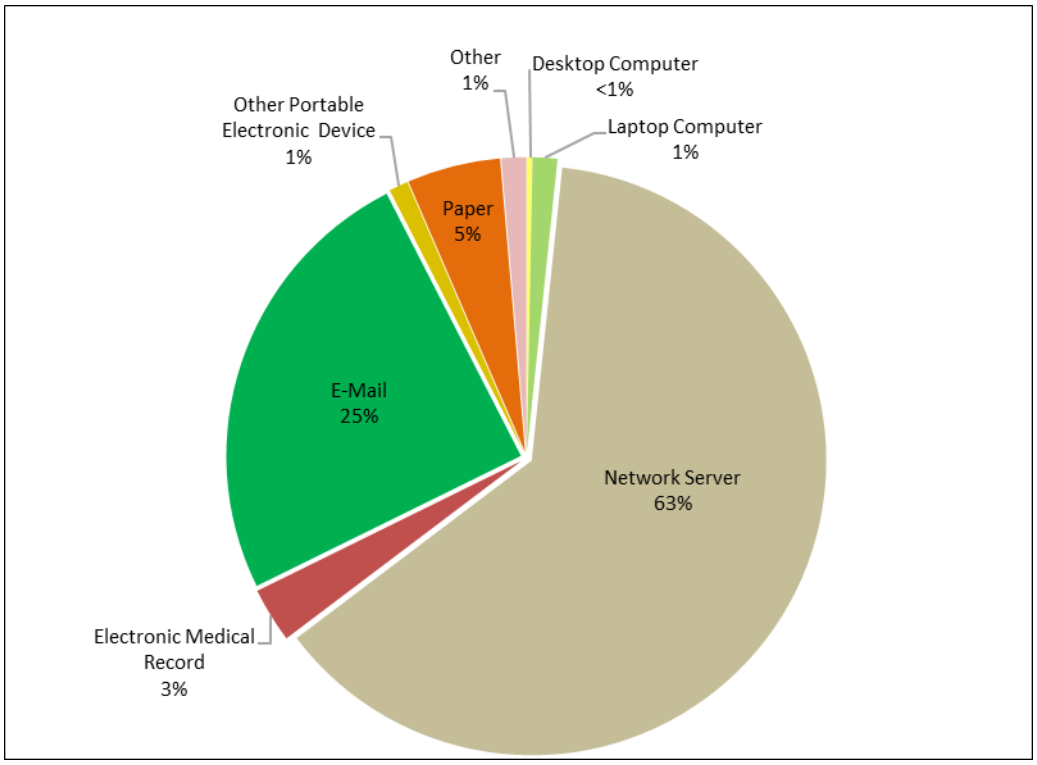

Figure 5

HHS Office for Civil Rights
Reports of Breaches of Unsecured PHI Affecting 500 or More Individuals in 2024 by Percentage of Affected Individuals for each Location of PHI

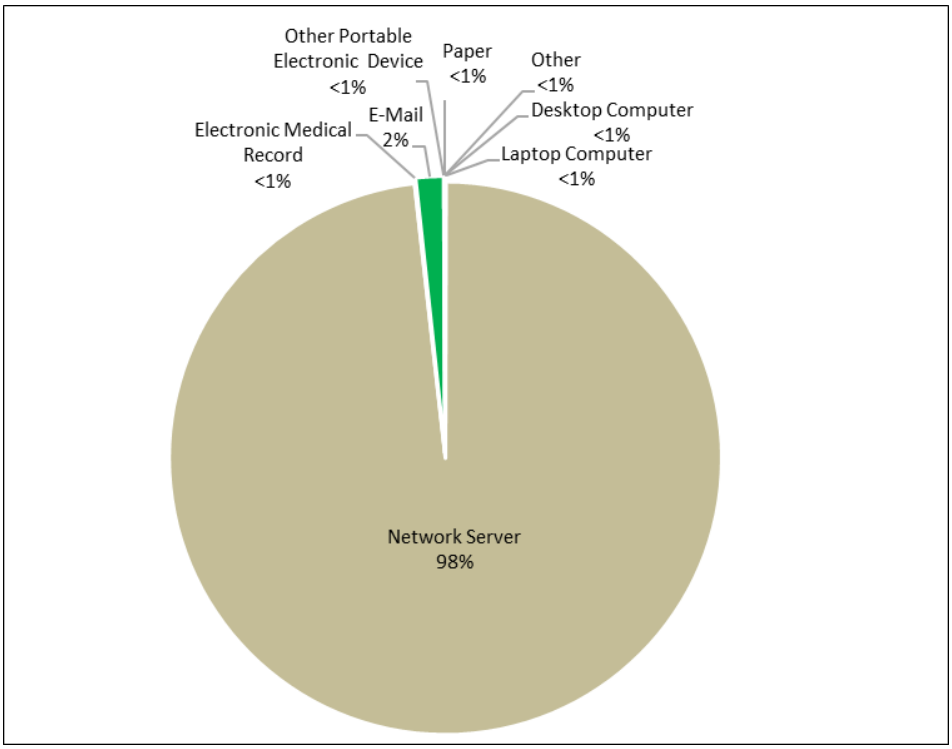

Figure 6

Largest breaches in 2024 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 2024 resulted from a hacking/IT incident in which hackers deployed ransomware that compromised the servers of a healthcare clearinghouse containing electronic PHI (ePHI). The breach incident affected approximately 192,000,000 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 reported breach of unsecured PHI in 2024 involving the unauthorized access or disclosure of ePHI affected approximately 483,126 individuals. In this case, a business associate reported that it inadvertently posted PHI on its website. Other incidents of unauthorized access or disclosure involved the tracking of ePHI using data tracking technology, PHI 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 2024 resulted from a

covered entity whose employees improperly disposed of medical records after the termination of the general manager. This breach affected approximately 8,000 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 2024 resulted from the theft of a cell phone belonging to a healthcare provider. The theft affected approximately 11,435 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 2024 resulted from the loss of a USB flash drive that was misplaced. The USB flash drive contained the PHI of 4,265 individuals. Other incidents in this category involved paper and other electronic media that could not be located.

Remedial Action Reported

For breaches affecting 500 or more individuals that occurred in 2024, 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

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 2024, notification to OCR was required no later than March 1, 2025. OCR received 74,299 reports of breaches involving fewer than 500 individuals that occurred in calendar year 2024, which affected a total of approximately 340,618 individuals.

Breaches involving fewer than 500 individuals for 2024

For the 74,299 reports of breaches of unsecured PHI affecting fewer than 500 individuals, OCR received:

(1) 68,761 breach reports (93% of total breach reports) from health care providers affecting 272,139 individuals (80% of total affected individuals);
(2) 3,933 breach reports (5% of total breach reports) from health plans affecting 30,384 individuals (9% of total affected individuals);
(3) 1,500 breach reports (2% of total breach reports) from business associates affecting 29,221 individuals (9% of total affected individuals); and
(4) 105 breach reports (<1% of total breach reports) from health care clearinghouses affecting 8,874 individuals (3% 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 2024 by Percentage of Reports Received for each Entity Type

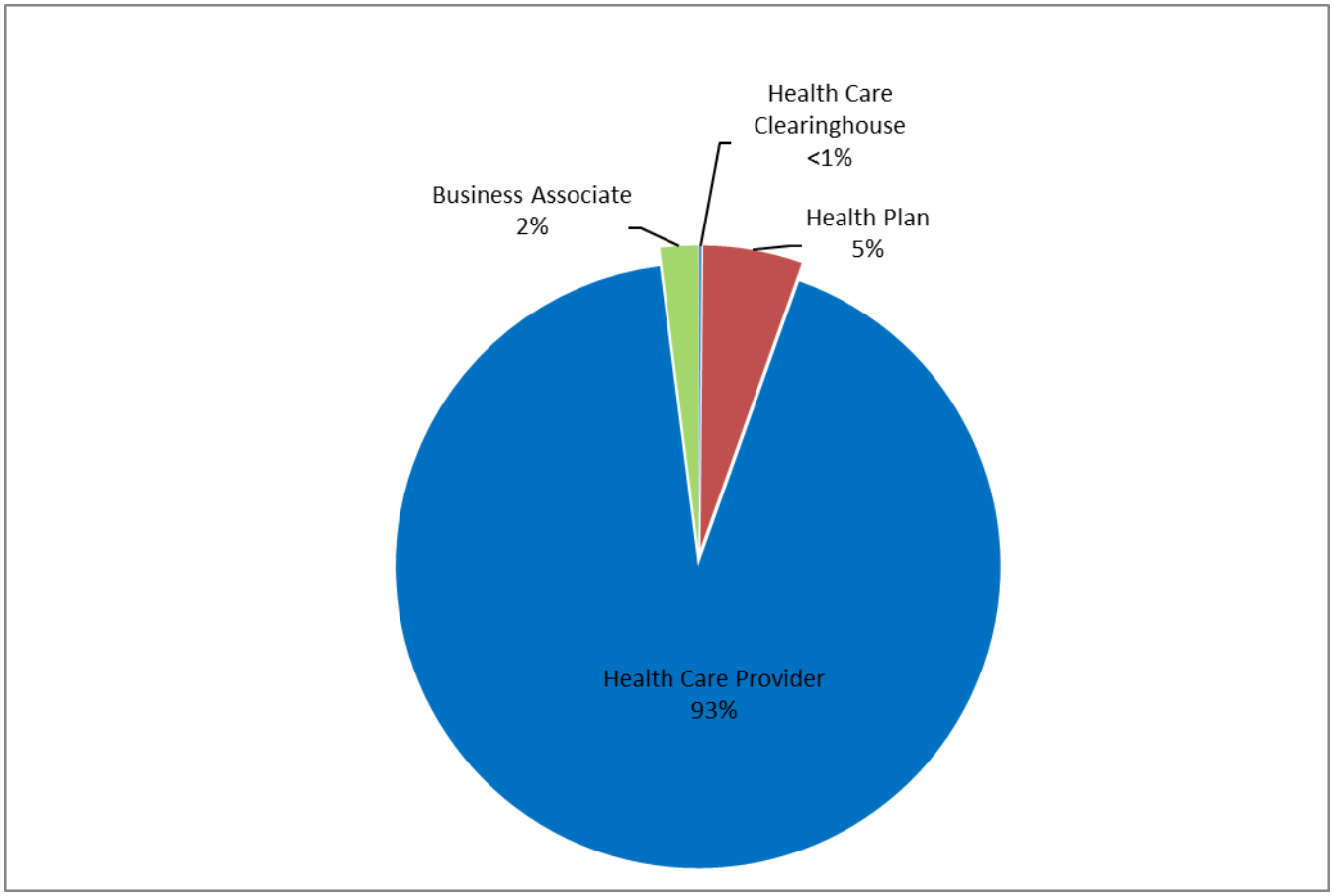

Figure 7

HHS Office for Civil Rights
Reports of Breaches of Unsecured PHI Affecting Fewer Than 500 Individuals in 2024 by Percentage of Affected Individuals for each Entity Type

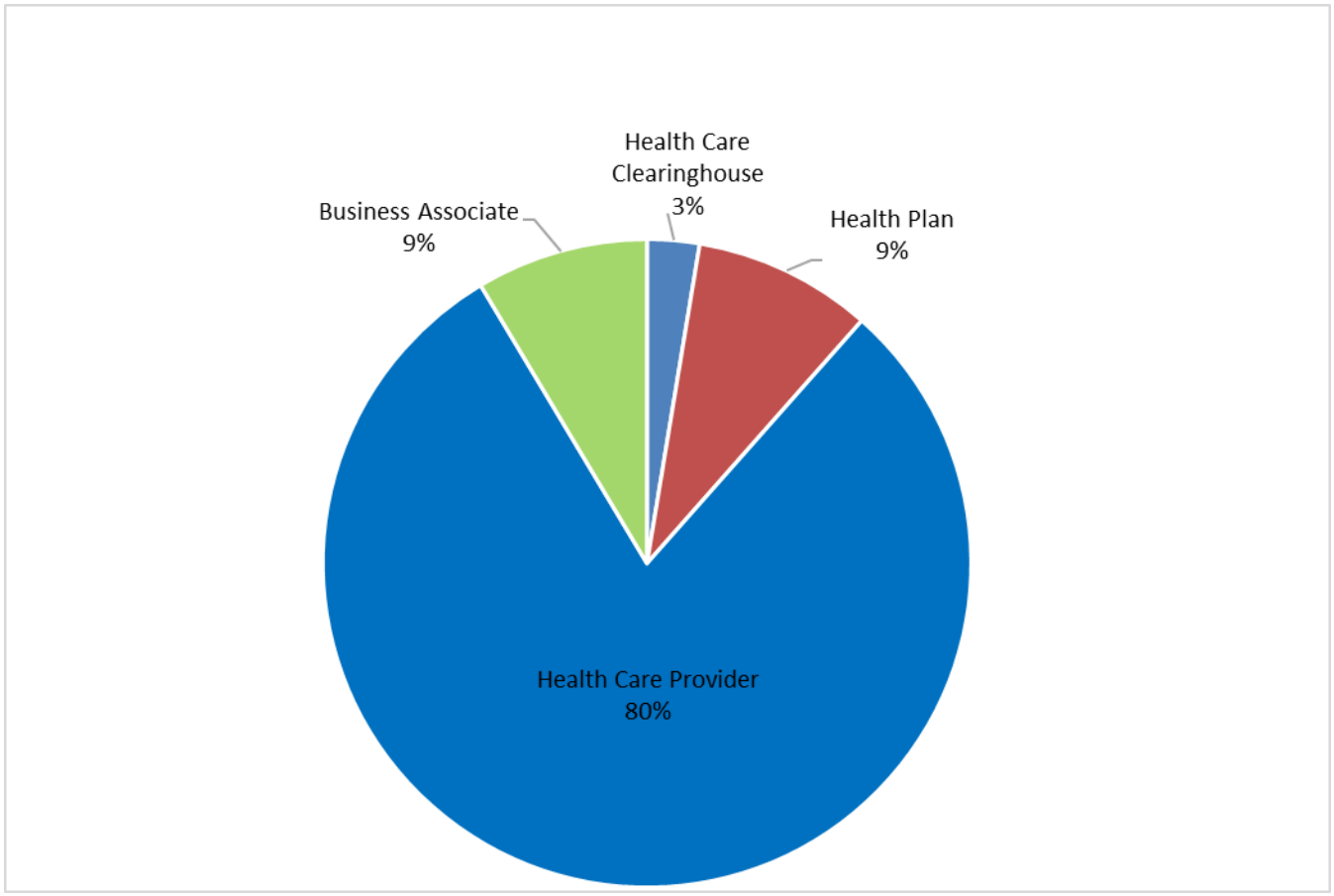

Figure 8

The 74,299 reports submitted to OCR for breaches of unsecured PHI affecting fewer than 500 individuals occurring in 2024 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 (69,773 breach reports (94% of total breach reports) affecting 196,567 individuals (58% of total affected individuals));
(2) Loss of electronic media or paper records containing PHI (2,593 reports (4% of total breach reports) affecting 11,217 individuals (3% of total affected individuals));
(3) Hacking/IT incident involving electronic equipment or a network server (885 reports (1% of total breach reports) affecting 76,693 individuals (23% of total affected individuals));
(4) Theft of electronic equipment/portable devices or paper containing PHI (822 reports (1% of total breach reports) affecting 49,991 individuals (15% of total affected individuals)); and
(5) Improper disposal of PHI (226 reports (<1% of total breach reports) affecting 6,150 individuals (2% of total affected individuals)).

See Figures 9 and 10.

[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 2024 by Percentage of Reports Received for each Type of Breach

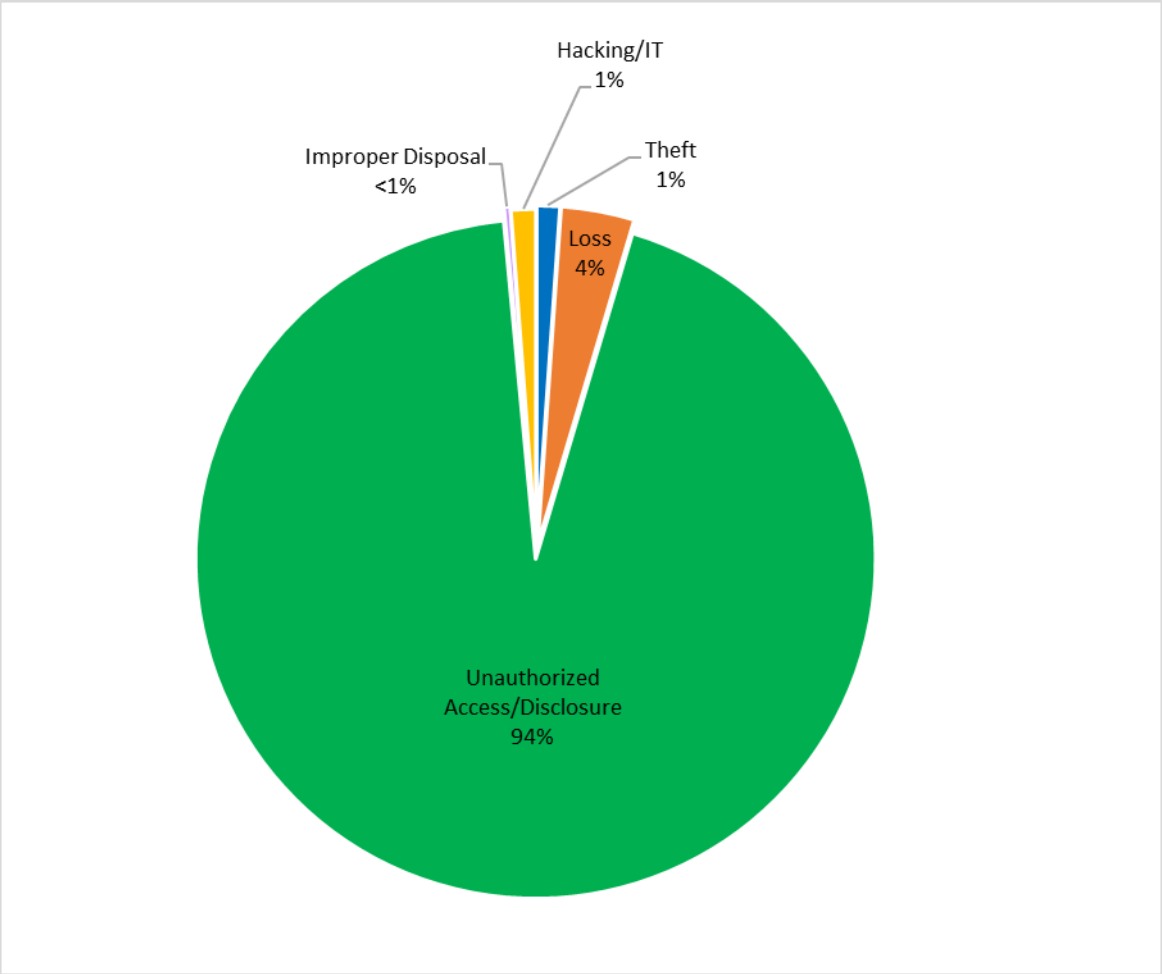

Figure 9

HHS Office for Civil Rights
Reports of Breaches of Unsecured PHI Affecting Fewer Than 500 Individuals in 2024 by Percentage of Affected Individuals for each Type of Breach

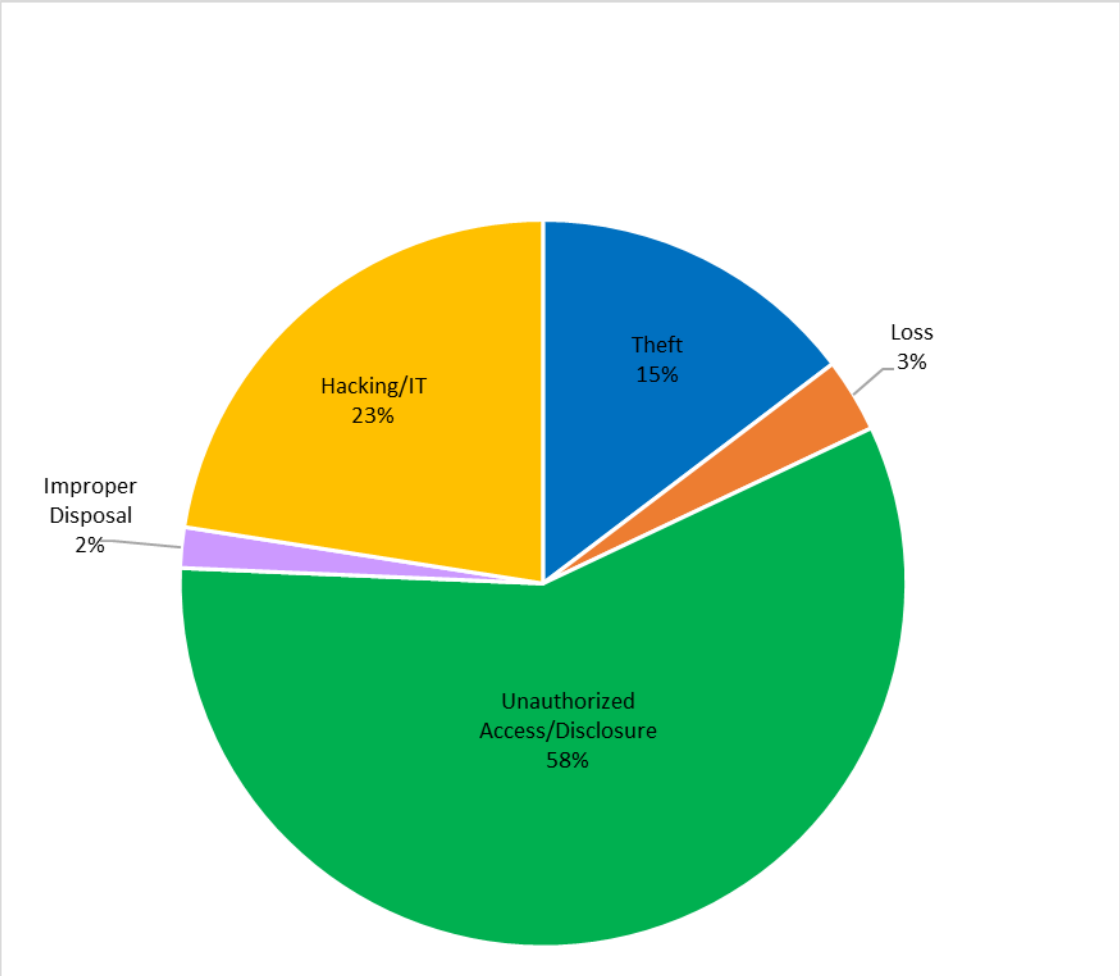

Figure 10

The 74,299 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 (44,304 reports (60% of total breach reports) affecting 94,760 individuals (28% of total affected individuals));
(2) Electronic medical record (EMR) (15,209 reports (20% of total breach reports) affecting 44,084 individuals(13% of total affected individuals));
(3) Other (7,438 reports (10% of total breach reports) affecting 27,870 individuals (8% of total affected individuals));[23]
(4) E-mail (4,373 reports (6% of total breach reports) affecting 86,314 individuals (25% of total affected individuals));
(5) Desktop computer (1,133 reports (2% of total breach reports) affecting 11,335 individuals (3% of total affected individuals));
(6) Other portable electronic device (1,001 reports (1% of total breach reports) affecting 5,872 individuals (2% of total affected individuals));
(7) Network server (612 reports (1% of total breach reports) affecting 65,517 individuals (19% of total affected individuals)); and
(8) Laptop computer (229 reports (< 1% of total breach reports) affecting 4,866 individuals (1% 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 2024 by Percentage of Reports Received for each Location of PHI

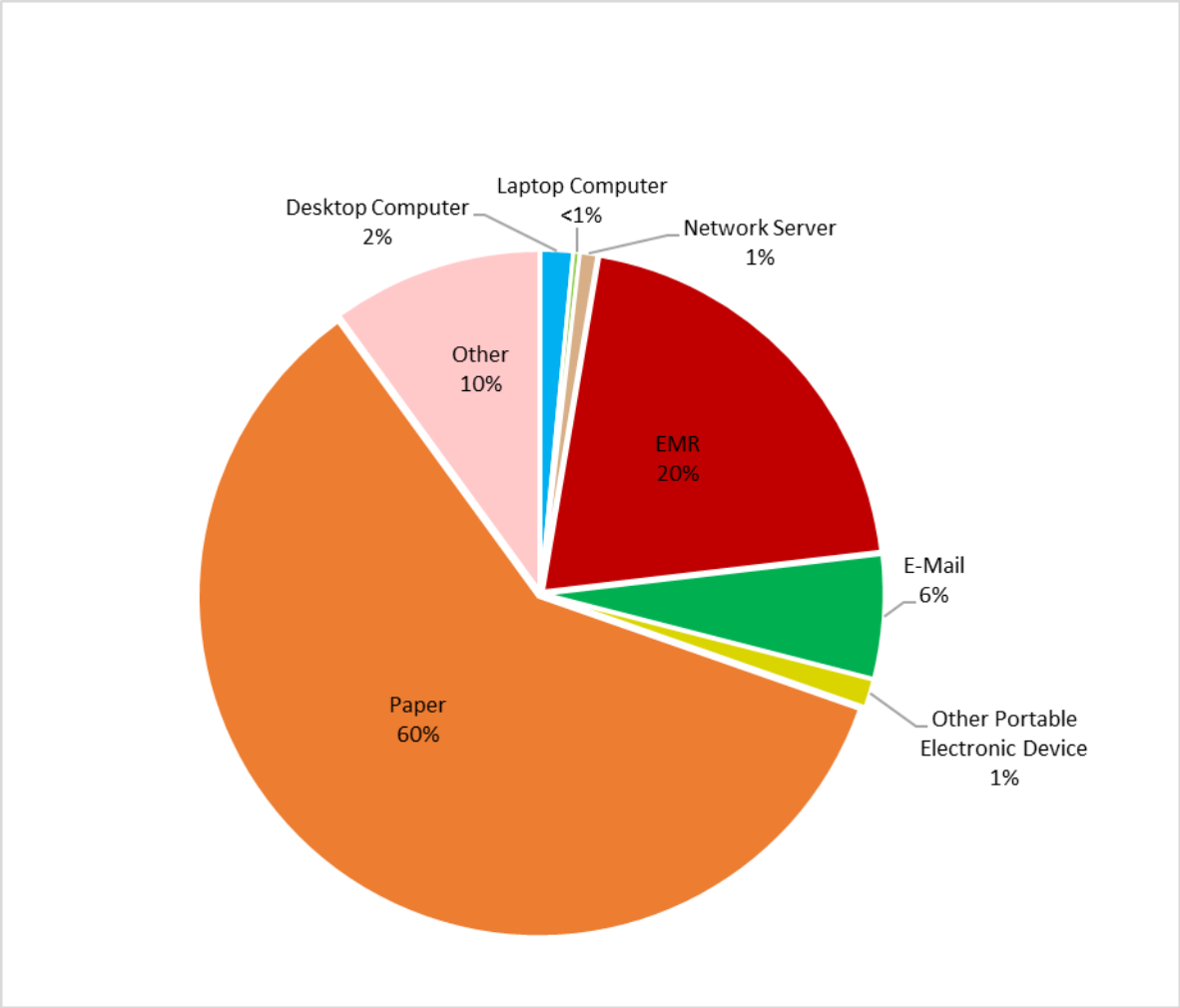

Figure 11

HHS Office for Civil Rights
Reports of Breaches of Unsecured PHI Affecting Fewer Than 500 Individuals in2024 by Percentage of Affected Individuals for each Location of PHI

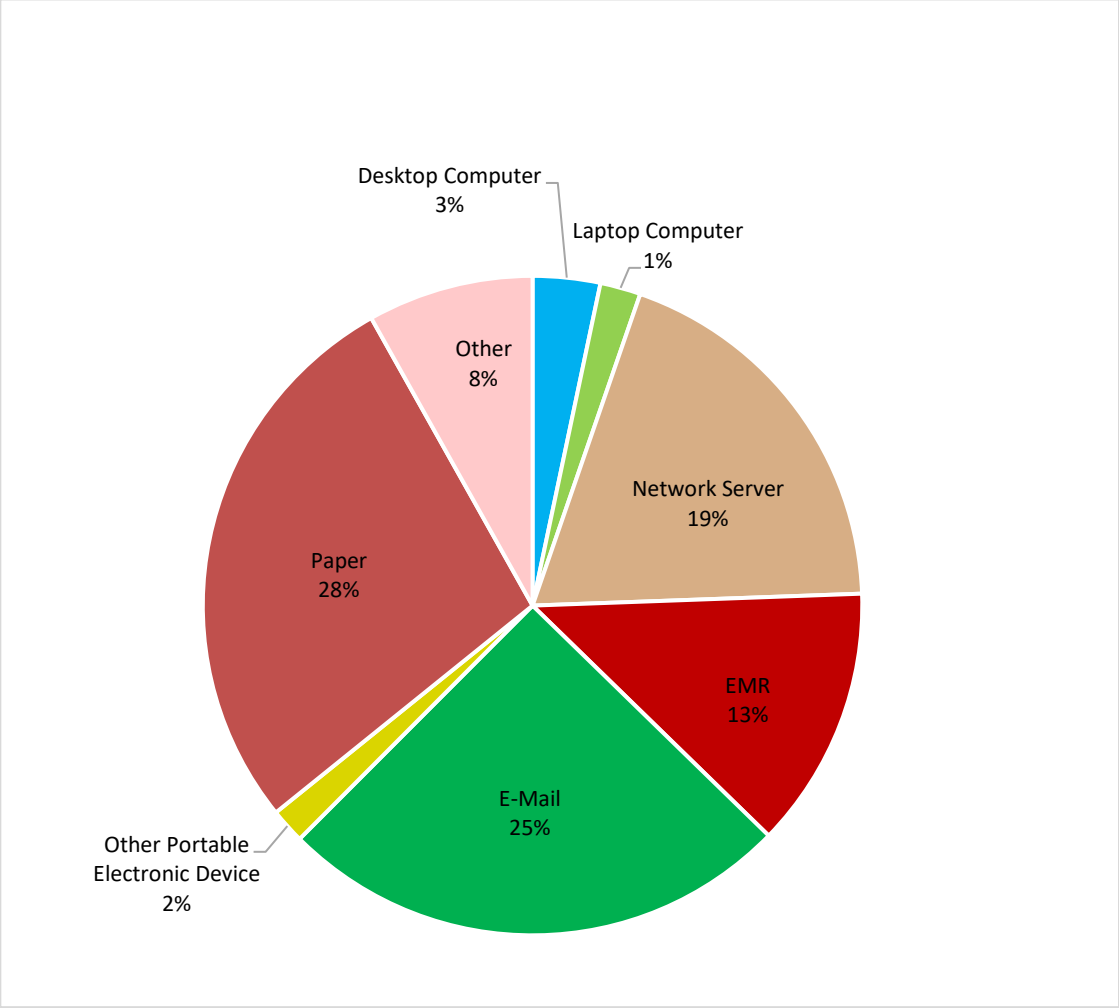

Figure 12

Details on breaches involving fewer than 500 individuals for 2024

As in previous years, breach incidents reported for 2024 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, many breach reports for 2024 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 two breach investigations involving fewer than 500 individuals in 2024.

Cases Investigated and Action Taken

OCR opened investigations into all 663 reported breaches affecting 500 or more individuals that occurred in 2024. OCR also opened two investigations into breaches affecting fewer than 500 individuals. OCR completed 785 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 2024 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 2024*.

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 and enforcement activities in 2024 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 2024 include:
    - Risk Analysis.[25] Security Rule investigations and enforcement actions in 2024 continue to find significant areas of non-compliance with the Security Rule's risk analysis provision. The Security Rule requires regulated entities

[24] 45 CFR164.308(a)(1).
[25] 45 CFR 164.308(a)(1)(ii)(A).

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. Risk analysis materials submitted to OCR for review frequently lacked thoroughness leading to gaps in the identification and assessment of risks to the regulated entity's ePHI. Examples of such gaps include assessments focused mainly on business administration applications that process ePHI rather than a taking more holistic view of risks to ePHI as it flows throughout the organization (*e.g.*, risks to ePHI from clinical and infrastructure systems; database, web, email, and backup servers; legacy systems). Without an accurate and comprehensive understanding of risks to their ePHI, regulated entities struggle to protect ePHI and remain vulnerable to cyberattacks and breaches of ePHI.

- Risk Management.[26] Implementation of security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level is also required by the Security Rule. However, OCR's investigations continue to find regulated entities not in compliance with this requirement. Risk management deficiencies include failures to implement security measures to reduce risks as well as implementing security measures that do not reduce risk to a reasonable and appropriate level. For example, an attacker accessing ePHI remotely using the compromised password of a workforce member is a high risk for many regulated entities. Yet it was often the case in 2024 that OCR's investigations found that it was only after a breach had occurred that a regulated entity implemented an authentication solution, such as multi-factor authentication, sufficient to reduce such risk.

- Information System Activity Review.[27] Regular review of records of information system activity, such as audit logs, access reports, and security incident tracking reports, is required by the Security Rule. Deficiencies found during OCR's investigations and enforcement activities in 2024 included failures to review records of any information system activity, reviewing records only in response to a breach or other security incident, and reviewing records on an infrequent, ad-hoc basis (*i.e.*, not a regular review). Regular review of information system activity records is an important part of a regulated entity's proactive cybersecurity and Security Rule compliance posture. Such reviews help regulated entities understand a baseline of system activity within their organization that can help detect anomalous behavior that could indicate a breach or security incident.

- Access Control Standard.[28] The Security Rule requires regulated entities to implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to persons or software programs authorized for such access. Ensuring that technical controls are in place to prevent unauthorized access to ePHI is a critical component to prevent breaches of ePHI. However, OCR's investigations and enforcement activities in 2024 found numerous instances of potential non-compliance

[26] 45 CFR 164.308(a)(1)(ii)(B).
[27] 45 CFR 164.308(a)(1)(ii)(D).
[28] 45 CFR 164.312(a).

with this standard. OCR found instances where, once an attacker had gained access to a regulated entity's network, there were few if any controls in place preventing the attacker from accessing various information systems within the regulated entity's environment including information systems maintaining ePHI. In other instances, OCR found excessive *(i.e.*, administrator) privileges granted to generic (*i.e.*, non-unique) shared accounts that, once compromised by an attacker, could be used to circumvent access controls protecting ePHI. Access controls that prevent, or at least impede, an attacker's access to information systems and the ability to escalate privileges are important tools in every regulated entity's cybersecurity toolbox. Effective access controls can prevent unauthorized access to ePHI, thus lessening the potential impact of a breach.

- Person or Entity Authentication.[29] Regulated entities are required, in accordance with the Security Rule, to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed. OCR's investigations in 2024 found that compromised credentials (*i.e.*, a password or other login credentials known to an attacker) continue to be one of the main attack vectors by which attackers gain unauthorized access to a regulated entity's network and information systems. OCR's investigations and enforcement activities found weak authentication practices of regulated entities that led to breaches included the use of weak passwords, including weak passwords on accounts with administrator privileges; system accounts using default passwords; and single-factor remote access solutions. Multi-factor authentication, especially when used to secure remote access, can help limit unauthorized access to a regulated entity's network. OCR published a cybersecurity newsletter in 2023 strongly advocating that regulated entities consider multi-factor authentication as an authentication solution to better secure access to ePHI and to meet HIPAA's authentication requirement.

Summary and Conclusion

In 2024, Hacking/IT incidents was the largest category of breaches of unsecured PHI affecting 500 or more individuals (81% of the reports received and 99% of the individuals affected). Network servers remained the largest category by location for breaches affecting 500 or more individuals (63% of the reports received and 98% of the individuals affected). For the breaches affecting fewer than 500 individuals, unauthorized access or disclosure was the largest category of type of breach reported (94%), and paper records was the largest by location (60%).

The breach notification requirements increase transparency of breaches both with the public 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 individuals affected, date of breach, type of breach, and location of the breached information (*e.g.*, laptop computer).

[29] 45 CFR 164.312(d).

Additionally, the website provides brief summaries of the enforcement cases, including breach report investigations, that OCR has investigated and closed.

In 2024, OCR continued 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 2024, OCR resolved twelve breach investigations with resolution agreements/corrective action plans and civil money penalties and collected settlements totaling over $7.8 million.

APPENDIX

Resolution Agreements and Civil Money Penalties[30] in 2024

Resolution Agreement with Plastic Surgery Associates of South Dakota

Plastic Surgery Associates of South Dakota (PSA) paid $500,000 and agreed to take corrective actions to settle potential violations of the HIPAA Security Rule. OCR initiated an investigation following the receipt of a breach report filed in July 2017, which reported that it discovered that nine workstations and two servers were infected with ransomware, affecting the PHI of 10,229 individuals.

OCR's investigation revealed multiple potential violations of the HIPAA Security Rule, including failures to conduct a compliant risk analysis to determine the potential risks and vulnerabilities to PHI in its systems; implement security measures sufficient to reduce the risks and vulnerabilities to PHI to a reasonable and appropriate level; implement procedures to regularly review records of information system activity; and implement policies and procedures to address security incidents.

This settlement occurred in May 2024. In addition to the monetary settlement, PSA agreed to:

- Conduct an accurate and thorough risk analysis to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its ePHI;
- 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.

.

Civil Money Penalty imposed on Providence Medical Institute

OCR imposed a civil money penalty of $240,000 against Providence Medical Institute (PMI). PMI is a non-profit physician services organization with 200 providers across 32 medical offices, including seven urgent care centers throughout California.

OCR initiated an investigation following the receipt of a breach report filed by PMI in April 2018, which reported that its systems were impacted by a series of ransomware attacks that affected the ePHI of 85,000 individuals between February and March 2018. OCR's investigation determined that servers containing ePHI were encrypted with ransomware three times. OCR found two potential

[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 2023.

violations of the HIPAA Security Rule, including failure to have a business associate agreement in place and failure to implement policies and procedures to allow only authorized persons or software programs access to ePHI.

In March 2024, OCR issued a Notice of Proposed Determination seeking to impose a civil money penalty. Providence Medical Institute waived its right to a hearing and did not contest OCR's findings. Accordingly, in July 2024, OCR issued a Notice of Final Determination and imposed a civil money penalty of $240,000.

Resolution Agreement with Bryan County Ambulance Authority

Bryan County Ambulance Authority (BCAA) paid $90,000 and agreed to take corrective actions to settle a potential violation of the HIPAA Security Rule. BCAA provides emergency medical services in Oklahoma.

OCR began investigating BCAA in May 2022 after it filed a breach report stating that it experienced a ransomware attack that encrypted its network and compromised the PHI of 14,273 individuals. OCR's investigation found that BCAA had failed to conduct a compliant risk analysis to determine the potential risks and vulnerabilities to ePHI in BCAA's systems.

This settlement occurred in July 2024. In addition to the monetary settlement, BCAA agreed to:

- Conduct an accurate and thorough risk analysis to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its ePHI;
- 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; and
- Train workforce members on the policies and procedures for the privacy and security of PHI.

Civil Money Penalty imposed on Children's Hospital Colorado

OCR imposed a civil money penalty of $548,265 against Children's Hospital Colorado (CHC). CHC is a children's hospital headquartered in Aurora, Colorado.

OCR launched an investigation after receiving breach reports in 2017 and 2020 regarding email phishing and cyberattacks. These breach incidents compromised one email account containing the PHI of 3,370 individuals and three additional email accounts containing the PHI of 10,840 individuals. OCR's investigation determined that the first reported breach occurred because multi-factor authentication was disabled, and the second breach occurred when workforce members gave permission to unknown third parties to access their email accounts. OCR also found violations of the HIPAA Privacy Rule for failure to train workforce members on the HIPAA Privacy Rule, and the HIPAA Security Rule requirement to conduct a compliant risk analysis to determine the potential risks and vulnerabilities to PHI in its computer systems.

In June 2024, OCR issued a Notice of Proposed Determination seeking to impose a civil money penalty. Children's Hospital Colorado waived its right to a hearing and did not contest OCR's findings. Accordingly, in September 2024, OCR issued a Notice of Final Determination and imposed a civil money penalty of $548,265.

Civil Money Penalty imposed on Gulf Coast Pain Management Consultants

OCR imposed a civil money penalty of $1,190,000 against Gulf Coast Pain Management Consultants (Gulf Coast). Gulf Coast is a pain management medical practice with 126 employees with locations in Alabama, Florida, Delaware, Maryland, New Jersey, and Pennsylvania.

OCR initiated an investigation following the receipt of a breach report in April 2019 by Gulf Coast which reported that a former contractor had impermissibly accessed Gulf Coast's electronic medical record system. OCR's investigation determined that the impermissible access occurred on three occasions, affecting approximately 34,310 individuals. The compromised PHI included patient names, addresses, phone numbers, email addresses, dates of birth, Social Security numbers, chart numbers, insurance information, and primary care information. OCR found four violations by Gulf Coast of the HIPAA Security Rule, including failures to:

- Conduct an accurate and thorough risk analysis to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its ePHI;
- Implement procedures to regularly review records of activity in information systems;
- Implement procedures to terminate former workforce members' access to ePHI; and
- Implement procedures for establishing and modifying workforce members' access to information systems.

In August 2024, OCR issued a Notice of Proposed Determination seeking to impose a civil money penalty. Gulf Coast waived its right to a hearing and did not contest OCR's findings. Accordingly, in September 2024, OCR issued a Notice of Final Determination and imposed a civil money penalty of $1,190,000.

Resolution Agreement with Elgon Information Systems

Elgon Information Systems (Elgon) paid $80,000 and agreed to take corrective actions to settle potential violations of the HIPAA Security Rule. Elgon is a company that provides electronic medical records and billing support services and is located in Massachusetts.

In June 2023, Elgon filed a breach report stating that approximately 31,248 individuals were affected when Elgon's computer system was infected with ransomware. OCR's investigation determined that Elgon failed to conduct an accurate and thorough risk analysis to determine the potential risks and vulnerabilities to ePHI in its computer system.

This settlement occurred in November 2024. In addition to a monetary settlement, Elgon agreed to:

- Review and update its risk analysis to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its ePHI;

- 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.

Resolution Agreement with Virtual Private Network Solutions

Virtual Private Network Solutions (VPNS) paid $90,000 and agreed to take corrective actions to settle potential violations of the HIPAA Security Rule. VPNS provides data hosting, cloud services, and user and application support to covered entities and business associates. It is based in Richmond, Virginia.

In December 2021, OCR received a breach report from VPNS stating that it experienced a ransomware incident that impacted portions of its server infrastructure. OCR's investigation determined that VPNS failed to conduct a compliant risk analysis to determine the potential risks and vulnerabilities to ePHI in their system.

This settlement occurred in November 2024. In addition to the monetary settlement, VPNS agreed to:

- Conduct an accurate and thorough risk analysis to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its ePHI;
- Implement a risk management plan to address and mitigate security risks and vulnerabilities identified in its risk analysis;
- Develop, maintain, and revise, as necessary, its written policies and procedures to comply with the HIPAA Rules; and
- Conduct a breach risk assessment of the October 31, 2021, breach and provide evidence to OCR that all covered entities affected by the breach have been notified of the breach and the identity of individuals affected by the breach.

Resolution Agreement with Northeast Surgical Group

Northeast Surgical Group (NESG) paid $10,000 and agreed to take corrective actions to settle potential violations of the HIPAA Security Rule. NESG provides surgical care in Michigan.

In March 2023, OCR received a breach report concerning a ransomware incident that had affected NESG's information system. NESG concluded that the ePHI of 15,298 patients had been encrypted and exfiltrated from its network. OCR's investigation determined that NESG had failed to conduct a compliant risk analysis to determine the potential risks and vulnerabilities to ePHI in NESG's systems.

This settlement occurred in November 2024. In addition to the monetary settlement, NESG agreed to:

- Conduct an accurate and thorough risk analysis to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI;
- Implement a risk management plan to address and mitigate security risks and vulnerabilities identified in the risk analysis;
- Develop, maintain, and revise, as necessary, its written policies and procedures to comply with the HIPAA Rules; and
- Train workforce members on the policies and procedures for the privacy and security of PHI.

Resolution Agreement with USR Holdings

USR Holdings (USR) paid $337,750 and agreed to take corrective actions to settle potential violations of the HIPAA Security Rule. USR is located in Florida and provides administrative oversight and support services as a HIPAA business associate.

In February 2019, OCR initiated an investigation after receiving a breach report from USR Holdings stating that it experienced a cyberattack that compromised the PHI of 2,903 individuals. OCR's investigation found that USR failed to conduct an accurate and thorough risk analysis to identify vulnerabilities to the confidentiality, integrity, and availability of ePHI, failed to implement procedures for reviewing records of information system activities, failed to establish procedures to create and maintain retrievable exact copies of ePHI, and failed to prevent the unauthorized access and deletion of ePHI.

This settlement occurred in December 2024. In addition to the monetary settlement, USR agreed to:

- Conduct an accurate and thorough risk analysis to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI;
- Implement a risk management plan to address and mitigate security risks and vulnerabilities identified in the risk analysis;
- Develop a process to evaluate any environmental or operational changes that affect the security of PHI;
- Develop, maintain, and revise, as necessary, its written policies and procedures to comply with the HIPAA Rules; and
- Train workforce members on the policies and procedures for the privacy and security of PHI.

Resolution Agreement with Solara Medical Supplies

Solara Medical Supplies (Solara) paid $3,000,000 and agreed to take corrective actions to settle potential violations of the HIPAA Security and Breach Notification Rules. Solara provides medical supplies to individuals with diabetes in California.

In November 2019, OCR received a breach report concerning a phishing attack in which an unauthorized third party gained access to eight of Solara's employees' email accounts between April and June 2019, resulting in the breach of 114,007 individuals' ePHI. In January 2020, OCR received notification of a second breach, when Solara reported that it had sent 1,531 breach

notification letters to the wrong mailing addresses. OCR's investigation determined that Solara failed to conduct a compliant risk analysis to identify the potential risks and vulnerabilities to ePHI in Solara's systems; failed to implement security measures sufficient to reduce the risks and vulnerabilities to ePHI to a reasonable and appropriate level; and failed to provide timely breach notification to individuals, HHS, and the media.

This settlement occurred in December 2024. In addition to the monetary settlement, Solara agreed to:

- Conduct an accurate and thorough risk analysis to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI;
- Implement a risk management plan to address and mitigate security risks and vulnerabilities identified in the risk analysis;
- Develop, maintain, and revise, as necessary, its written policies and procedures to comply with the HIPAA Rules; and
- Train workforce members on the policies and procedures for the privacy and security of PHI.

Civil Money Penalty imposed on Warby Parker

OCR imposed a civil money penalty of $1,500,000 against Warby Parker. Warby Parker, headquartered in New York, is a manufacturer and online retailer of prescription and non-prescription eyewear.

In December 2018, OCR initiated an investigation following receipt of a breach report filed by Warby Parker. The report stated that in November 2018, Warby Parker became aware of unusual, attempted log-in activity on its website. Warby Parker reported that between September 25, 2018, and November 30, 2018, unauthorized third parties gained access to Warby Parker customer accounts by using usernames and passwords obtained from other, unrelated websites that were presumably breached. In September 2020, Warby Parker filed an addendum breach report, updating the number of individuals affected by the breach to 197,986. The compromised ePHI included customer names, mailing addresses, email addresses, certain payment card information, and eyewear prescription information. Warby Parker also filed subsequent breach reports (each breach report affecting fewer than 500 persons) in April 2020, and June 2022, following similar attacks.

OCR's investigation found evidence of three potential violations of the HIPAA Security Rule, including a failure to conduct an accurate and thorough risk analysis to identify the potential risks and vulnerabilities to ePHI in Warby Parker's systems, a failure to implement security measures sufficient to reduce the risks and vulnerabilities to ePHI to a reasonable and appropriate level, and a failure to implement procedures to regularly review records of information system activity.

In September 2024, OCR issued a Notice of Proposed Determination seeking to impose a CMP. Warby Parker waived its right to a hearing and did not contest OCR's imposition of a CMP. Accordingly, in December 2024, OCR issued a Notice of Final Determination and imposed a civil money penalty of $1,500,000.

Resolution Agreement with Health Fitness

Health Fitness paid $227,816 and agreed to take corrective actions to settle potential violations of the HIPAA Security Rule. Health Fitness is a business associate that provides wellness plans throughout the United States and is headquartered in Lake Forest, Illinois.

Between October 2018 and January 2019, Health Fitness filed four breach reports regarding a misconfiguration on its servers that exposed the PHI of approximately 4,304 individuals. OCR's investigation found that Health Fitness did not perform a risk analysis to determine vulnerabilities and risks to confidentiality, integrity, and availability of ePHI that it holds.

This settlement occurred in December 2024. In addition to the monetary settlement, Health Fitness agreed to:

- Annually update its risk analysis to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI;
- Develop and implement a risk management plan to address and mitigate security risks and vulnerabilities identified in the risk analysis;
- Implement a process for evaluating environmental and operational changes that affect the security of ePHI; and
- Develop, maintain, and revise, as necessary, certain written policies and procedures to comply with the HIPAA Rules.