Annual Report to Congress on Breaches of Unsecured Protected Health Information

For Calendar Year 2021

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 2021 calendar year. The Annual Report to Congress on Breaches of Unsecured Protected Health Information identifies the number and nature of breaches of unsecured protected health information (PHI) that were reported to the Secretary of HHS during the year and the actions taken in response to those breaches.

Summary
OCR received 609 notifications[1] of breaches affecting 500 or more individuals, representing a decrease of 7% from the number of reports received in calendar year 2020. These reported breaches affected a total of approximately 37,182,558 individuals. The most commonly reported category of breaches was hacking, and the largest breach of this type involved approximately 3,253,822 individuals. OCR also received 63,571 reports of breaches affecting fewer than 500 individuals, with unauthorized access or disclosure reported as the most frequent type of breach reported. These smaller breaches affected a total of 319,215 individuals.

OCR initiated investigations into all 609 breaches affecting 500 or more individuals, as well as 22 breaches involving fewer than 500 individuals. OCR completed 554 breach investigations, through the provision of technical assistance; achieving voluntary compliance through corrective action; resolution agreements and corrective action plans; or after determining no violation occurred. Specifically, OCR resolved two breach investigations with resolution agreements, corrective action plans, and monetary payments totaling $5,125,000.[2]

Recommendations
There is a continued need for regulated entities to improve compliance with the HIPAA Rules, In particular, the Security Rule standards[3] and implementation specifications[4] of risk analysis, risk management, information system activity review, audit controls, and access control were areas identified as needing improvement in 2021 OCR breach investigations.

As in previous years, hacking/IT incidents remained the largest category of breaches affecting 500 or more individuals occurring in 2021, and hacking/IT incidents also affected the most individuals, comprising 75% of the reported breaches. The largest category of breaches of 500 or more individuals by location was network servers. For breaches affecting fewer than 500

[1] This figure refers to the number of breaches affecting 500 or more individuals that occurred or ended in calendar year 2021. In comparison, in 2021, OCR received 714 breach reports via the HIPAA Breach Web Portal, but some of these breaches did not occur in 2021 (*e.g.*, breach occurred in 2020, and was reported to OCR in 2021).
[2] The two breach investigations resolved in 2021 were Excellus Health Plan and Peachstate Health Management dba AEON Clinical Laboratories.
[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".

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

Background

Section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5), requires covered entities under the 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 of Health and Human Services ("the Secretary") to prepare and submit to the Senate Committee on Finance, the Senate Committee on Health, Education, Labor, and Pensions, the House Committee on Ways and Means, and the House Committee on Energy and Commerce an annual report containing:

- The number and nature of breaches reported to the Secretary, and
- The actions taken in response to those breaches.

The following report provides the required information for the breaches reported to the Secretary that occurred in calendar year 2021.

Section 13402(h) of the HITECH Act defines "unsecured protected health information" as "protected health information that is not secured through the use of a technology or methodology specified by the Secretary in guidance" and mandates that the Secretary issue guidance specifying the technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized persons. The guidance issued by the Secretary identifies encryption and destruction processes as tested by the National Institute of Standards and Technology as the two technologies and methodologies for rendering PHI unusable, unreadable, or indecipherable to unauthorized persons.[5] Covered entities and business associates that encrypt or destroy PHI in accordance with the guidance are not required to provide notifications in the event of a breach of such information because such information is not considered "unsecured."

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

OCR is the office within HHS that is responsible foradministering 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, HHS

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

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[6]] which compromises the securityor privacy of the PHI." Under the Breach Notification Rule, unauthorized acquisition, access, use, or disclosure of PHI (that does not fall into one of the enumerated exceptions discussed below) is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment. This risk assessment must address at least the following factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person(s) who used the PHI or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated.[7]

Section 13400(1)(B) of the HITECH Act provides several exceptions to the definition of "breach." These exceptions are set forth in the regulations at 45 CFR § 164.402. Section 164.402 excludes as a breach: (1) any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or business associate, if made in good faith and within the scope of authority, and if it does not result in further impermissible use or disclosure; (2) any inadvertent disclosure of PHI by a person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received is not further impermissibly used or disclosed; and (3) a disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain the information.

Breach Notification Requirements

Following the discovery of a breach of unsecured PHI, covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain cases, the media. In the case of a breach of unsecured PHI at or by a business associate of a covered entity, the business associate must notify the covered entity of the breach.[8] 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.

---

[6] The Privacy Rule protects the privacy of the health information of individuals while permitting important uses and disclosures of the information, such as for treatment of an individual and payment for health care, for certain public health purposes, in emergency situations, and to the friends and family involved in the care of an individual.
[7] *See* 45 CFR § 164.402 (definition of a "breach").
[8] 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.

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 coveredentity 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.[9]

- **Media Notice**

For breaches involving more than 500 residents of a State or jurisdiction, a covered entity must notify prominent media outlets serving the State or jurisdiction. As with individual notice, this media notification must be provided without unreasonable delay and no later than 60 calendar days following the discovery of a breach. It must include the same information as that required for the individual notice.[10]

- **Notice to the Secretary**

In addition to notifying affected individuals and the media (where appropriate), a covered entity must notify the Secretary of breaches of unsecured PHI. If a breach involves 500 or more individuals, a covered entity must notify the Secretary at the same time the affected individuals

[9] *See* 45 CFR § 164.404.
[10] *See* 45 CFR § 164.406.

are notified of the breach.[11] If a breach involves fewer than 500 individuals, covered entities may submit reports of such breaches on an annual basis. Reports of breaches involving fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches were discovered.[12] Covered entities must notify the Secretary by filling out and electronically submitting a breach report form on the HHS website at 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) where a breach occurs at or by its business associate, a covered entity may, pursuant to agreement with its business associate(s), delegate the responsibility of providing the required notifications to the business associate that suffered the breach or to another of its business associates.[13]

Summary of Breach Reports

This report describes the types and numbers of breaches reported to OCR that occurred between January 1, 2021, and December 31, 2021, and describes actions taken by coveredentities and business associates in response to these breaches.

This report generally describes OCR investigations and enforcement actions with respect to the reported breaches. Additional information on OCR's compliance and enforcement efforts in other areas may be found in OCR's *Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance for the Calendar Year of 2021*. OCR opens compliance reviews to investigate all reported breaches affecting 500 or more individuals and may open compliance reviews into reported breaches affecting fewer than 500 individuals. As discussed in greater detail below, for 2021, in addition to requiring covered entities and business associates to take corrective action in hundreds of cases, OCR resolved two breach investigations with resolution agreements, corrective action plans, and monetary payments totaling $5,125,000.

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

As shown in the table below, the number of breaches reported to OCR continues to increase. Between 2017 and 2021, the number of breaches affecting fewer than 500 individuals increased 5% and the number of breaches affecting 500 or more individuals rose 58%.

Year	Under 500 Breaches Reported	500+ Breaches Reported	Percentage Change in Under500 Breaches Reported	Percentage Change in 500+Breaches Reported
2021	63,571	609	-4% decrease	-7% decrease
2020	66,509	656	6% increase	61% increase
2019	62,771	408	-.5% decrease	35% increase
2018	63,098	302	4.6% increase	-21.5% decrease
2017	60,332	385	-	-
2017 to 2021	5.4% increase	58.2% increase	-	-

Source: Current and previous Reports to Congress

Breaches Involving 500 or More Individuals

Notification to the Secretary of breaches involving 500 or more individuals must occur contemporaneously with notice to affected individuals. OCR received 609 reports of such breaches for calendar year 2021,[14] which affected a total of approximately 37,182,558 individuals.[15]

[14] HHS receives some reports where the breach occurred over a period of several years. For the purposes of this report, breach incidents spanning multiple years are included with the data for the last year in which the breach occurred (*e.g.,* a breach incident that continued from 2019 into 2021 would be reported with the 2021 figures).

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

Breaches in 2021 Affecting 500 or More Individuals[16]

For the 609 breaches affecting 500 or more individuals in 2021, OCR received:

(1) 437 reports (72%) of breaches from health care providers (affecting 24,389,630 individuals (66%));
(2) 93 reports (15%) of breaches from health plans (affecting 3,236,443 individuals (9%));
(3) 77 reports (13%) of breaches from business associates (affecting 9,554,023 individuals(26%)); and
(4) 2 reports (<1%) of breaches from health care clearinghouses (affecting 2,462 individuals (<1%)).

See Figures 1 and 2.

HHS Office for Civil Rights
Breach Reports of Unsecured PHI Affecting 500 or more Individuals in 2021 by Percentage of Reports Received by Entity Type

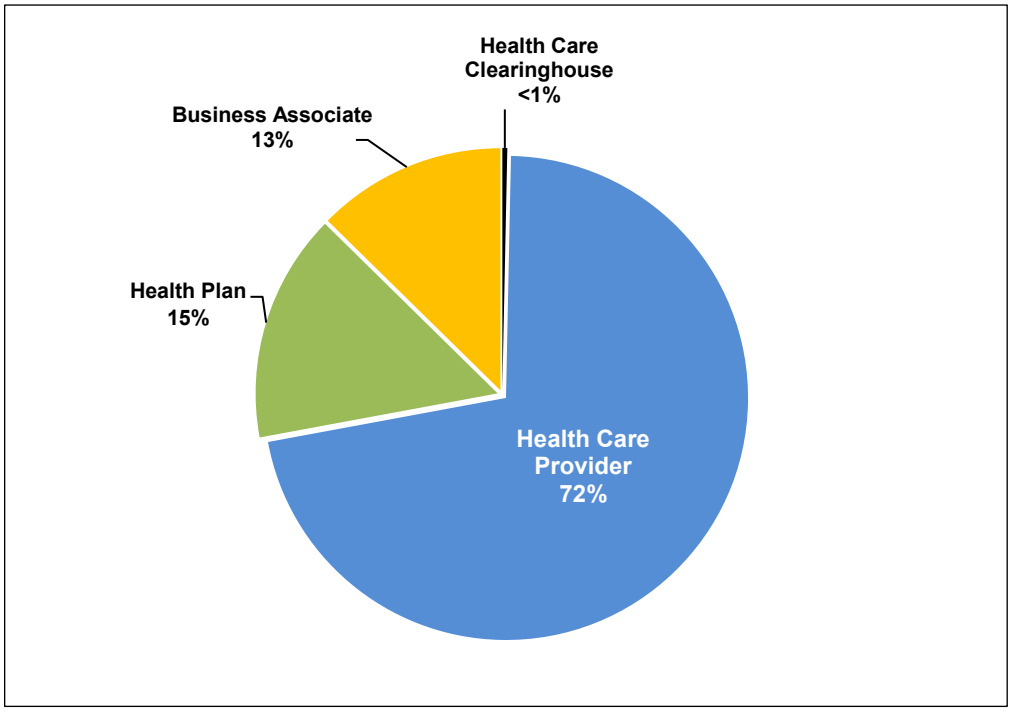

Figure 1

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

HHS Office for Civil Rights
Breach Reports of Unsecured PHI Affecting 500 or more Individuals in 2021 by Percentage of Individuals Affected by Entity Type

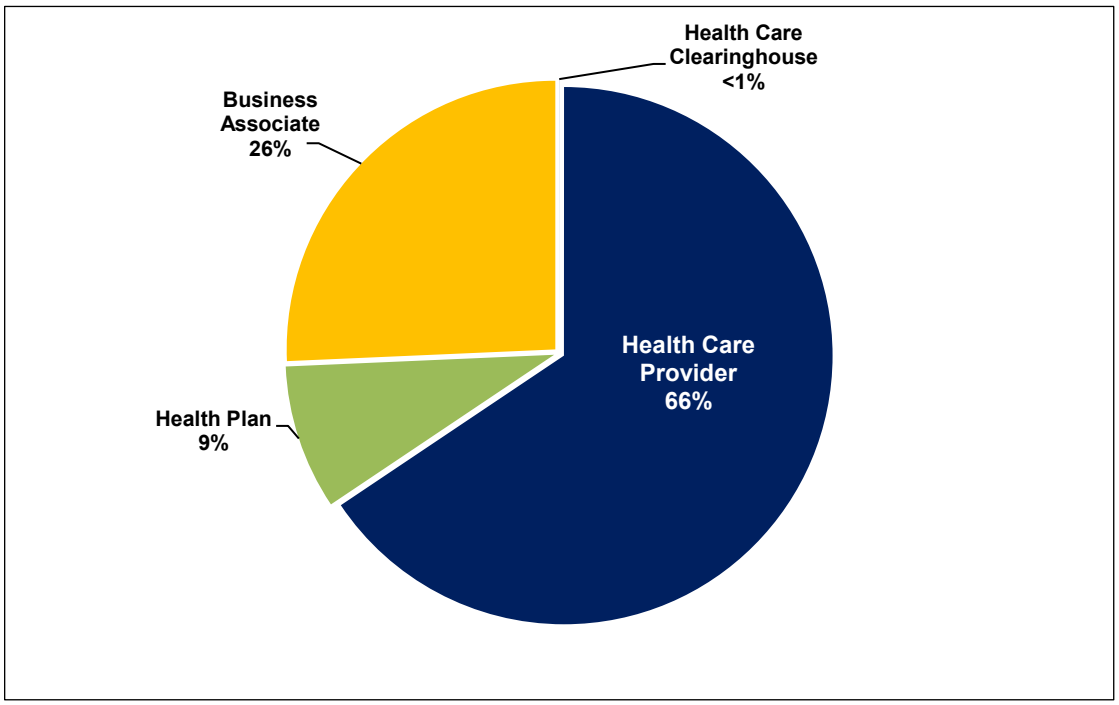

Figure 2

The 609 reports submitted to OCR for breaches affecting 500 or more individuals occurring in 2022 can be categorized by five general types or causes as follows (in order of frequency):[17]

(1) Hacking/IT incident of electronic equipment or a network server (459 reports (75%) affecting 35,264,773 individuals (95%));
(2) Unauthorized access or disclosure of records containing PHI (115 reports (19%) affecting 1,569,765 individuals (4%));
(3) Theft of electronic equipment/portable devices or paper containing PHI (21 reports (3%) affecting 123,615 individuals (<1%));
(4) Loss of electronic media or paper records containing PHI (9 reports (1%) affecting 33,845 individuals (<1%)); and
(5) Improper disposal of PHI (5 reports (1%) affecting 190,540 individuals (1%)).

See Figures 3 and 4.

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

HHS Office for Civil Rights
Breach Reports of Unsecured PHI Affecting 500 or more Individuals in 2021 by Percentage of Reports Received by Type of Breach

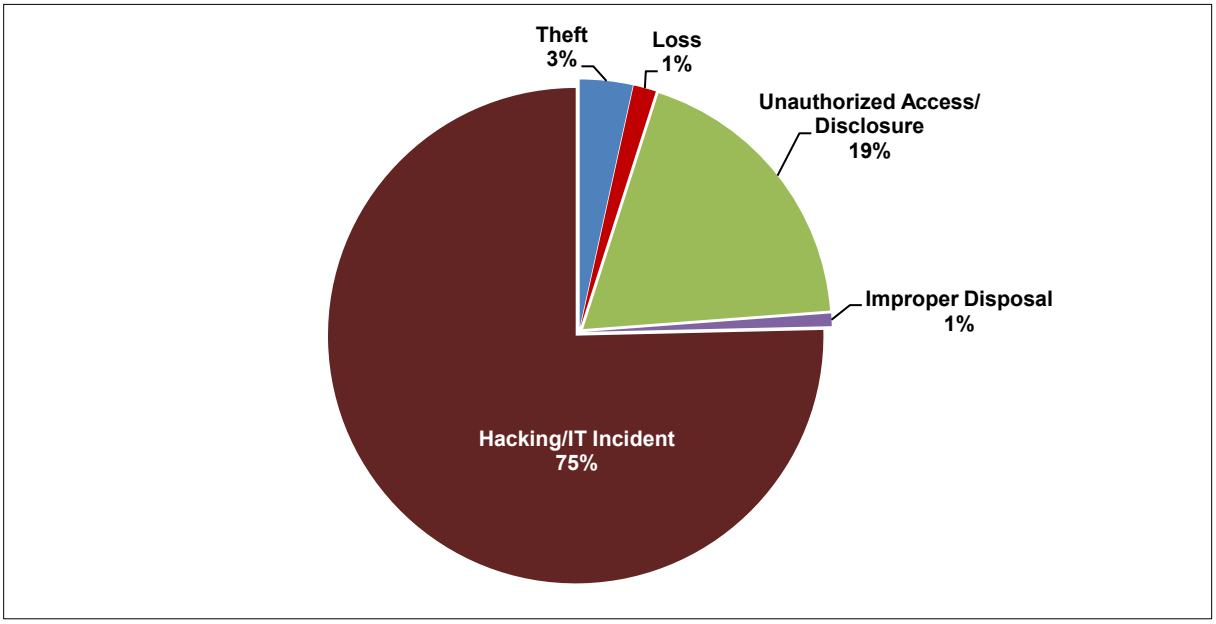

Figure 3

HHS Office for Civil Rights
Breach Reports of Unsecured PHI Affecting 500 or more Individuals in 2021 by Percentage of Individuals Affected by Type of Breach

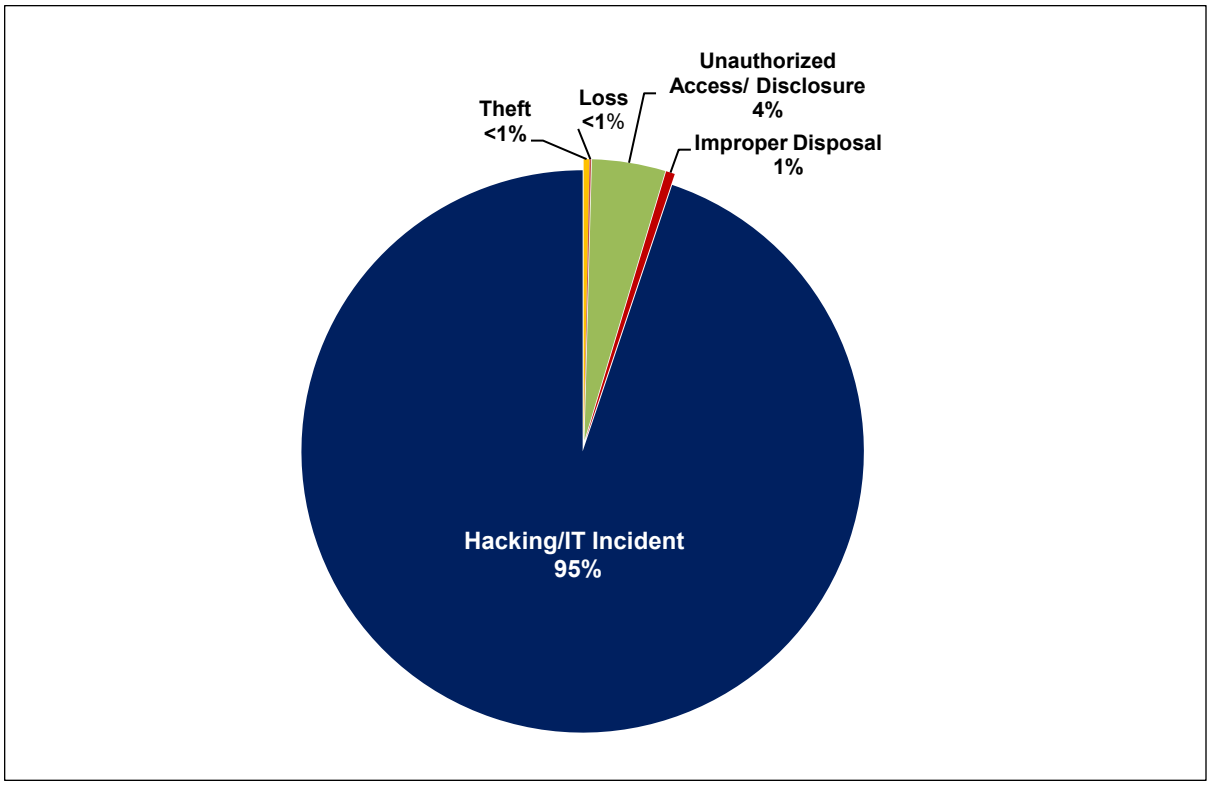

Figure 4

The 609 reports submitted to OCR for breaches occurring in 2021 described the following locations of the PHI (in order of frequency):[18]

(1) Network server (350 reports (57%), affecting 32,232,826 individuals (87%));
(2) E-mail (148 reports (24%) affecting 3,247,258 individuals (9%));
(3) Paper (42 reports (7%) affecting 158,672 individuals (<1%));
(4) Electronic medical record (23 reports (4%) affecting 454,555 individuals (1%));
(5) Desktop computer (17 reports (3%), affecting 678,288 individuals (2%))
(6) Other (15 reports (2%) affecting 329,726 individuals (1%));[19]
(7) Other portable electronic device (8 reports (1%) affecting 22,628 individuals (<1%)); and
(8) Laptop computer (6 reports (1%), affecting 58,605 individuals (< 1%)).

See Figures 5 and 6.

[18] A breach may occur in more than one location. The reporting entity selects the main location of the breach in compiling this data.
[19] Other is used when a covered entity is unable to identify the specific location of the breach, such as when an impersonator has accessed data, or data is taken by an employee, but the covered entity is not certain of the PHI's location when it was disclosed.

HHS Office for Civil Rights
Breach Reports of Unsecured PHI Affecting 500 or more Individuals in 2021 by Percentage of Reports Received by Location of PHI

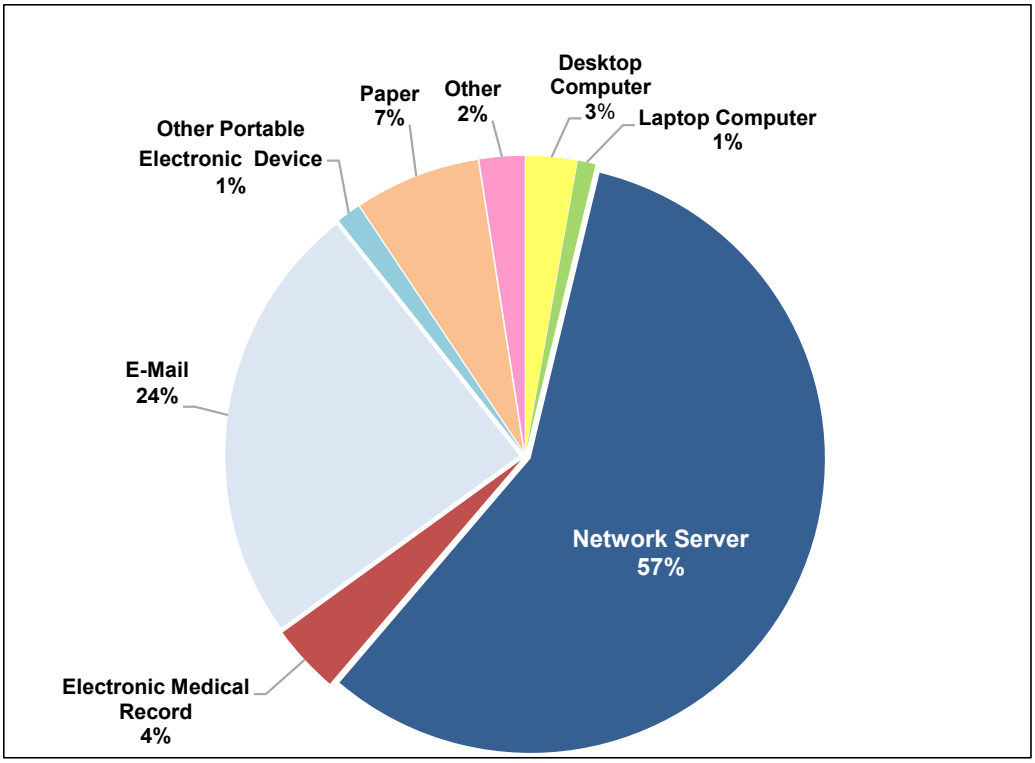

Figure 5

HHS Office for Civil Rights
Breaches of Unsecured PHI affecting 500 or More Individuals in 2021 by Percentage of Individuals Affected by Location of PHI

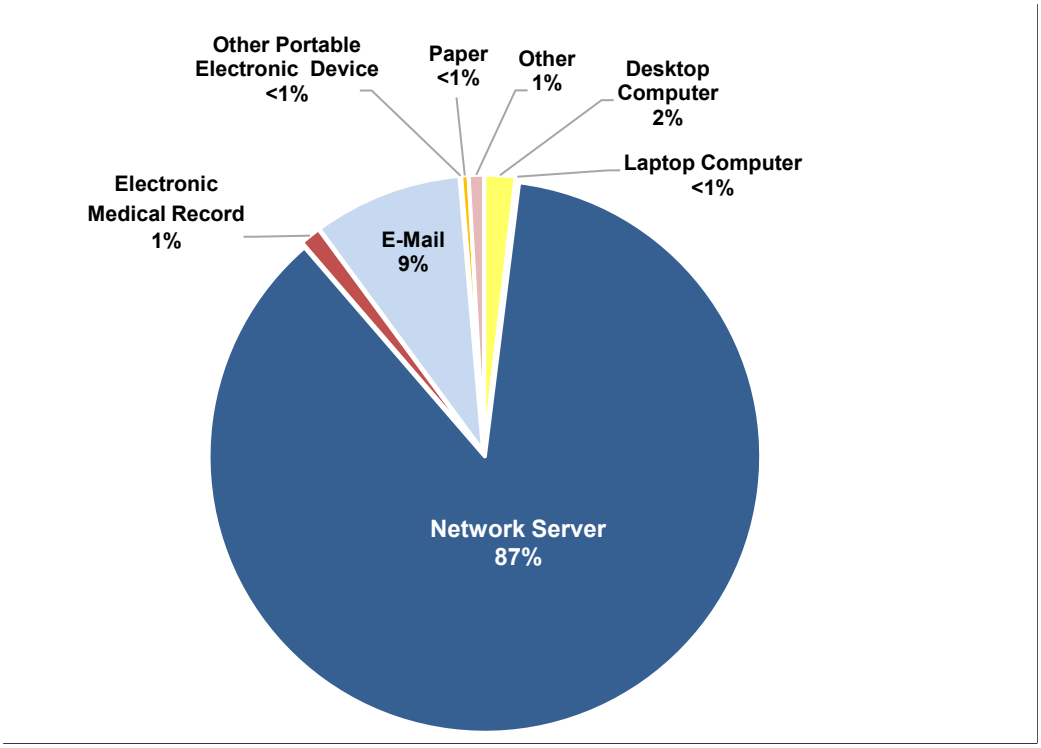

Figure 6

Largest breaches in 2021 for each reported cause

This section describes the largest breaches, by number of individuals affected, for each of the fivereported causes, followed by a short summary of scenarios reported for each cause.

Hacking/IT Incident of Electronic Equipment or Network Server: The largest breach in 2021 resulting from a hacking/IT incident in which two former employees hacked the server of a healthcare provider containing ePHI. The breach incident affected 3,253,822 individuals. Other hacking/IT incidents involved the use of malware, ransomware, phishing, and the posting of PHI to public websites.

Unauthorized Access or Disclosure of PHI: The largest breach in 2021 involving the unauthorized access or disclosure of ePHI affected approximately 326,417 individuals. A software configuration error exposed ePHI on a public website. Other incidents of unauthorized access or disclosure involved employees impermissibly accessing records outside the scope of their job responsibilities, and misdirected communications.

Improper Disposal: The largest reported improper disposal incident in 2021 resulted from a business associate who improperly disposed of hard drives containing ePHI by throwing them away in a dumpster. This breach affected 122,340 individuals. Other improper disposal

breaches involved disposing of paper records containing PHI in trash bins rather than authorized shred bins.

Theft: The largest theft-related breach in 2021 resulted from the theft of ePHI when a hospital was burglarized, and a network server was stolen. The theft affected approximately 21,601 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 2021 resulted from the loss of medical records that contained the PHI of approximately 14,532 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 2021, in addition to providing the required notifications, covered entities most commonly reported taking one or more of the following steps to mitigate the potential consequences of the breaches and to prevent future breaches:

- Implementing multi-factor authentication for remote access;
- Revising policies and procedures;
- Training or retraining workforce members who handle PHI;
- Providing free credit monitoring and identity theft protection services to customers;
- Adopting encryption technologies;
- Imposing sanctions on workforce members who violated policies and procedures for removing PHI from facilities or who improperly accessed PHI;
- Changing passwords;
- Performing a new risk assessment; and
- Revising business associate contracts to include more detailed provisions for the protection of health information.

Breaches Involving Fewer than 500 Individuals

A covered entity must notify OCR of breaches involving fewer than 500 individuals no later than 60 days after the end of the calendar year in which the breaches are discovered. For breaches discovered during 2021, notification to OCR was required no later than March 1, 2022.

Breaches involving fewer than 500 individuals for 2021

OCR received 63,571 reports of breaches affecting fewer than 500 individuals occurring in calendar year 2021. These smaller breaches affected 319,215 individuals. Set forth below are the breaches submitted to OCR by covered entity type (in order of frequency):

(1) Health Care Providers (57,974 reports (91%) affecting 240,442 individuals (75%));
(2) Health Plans (4,171 reports (7%) affecting 30,577 individuals (10%));
(3) Business Associates (1,383 reports (2%) affecting 48,081 individuals (15%)); and
(4) Health Care Clearinghouses (43 reports (<1%) affecting 115 individuals (<1%)).

See Figures 7 and 8.

HHS Office for Civil Rights
Breach Reports of Unsecured PHI affecting Fewer Than 500 Individuals in 2021 by Percentage of Reports Received by Entity Type

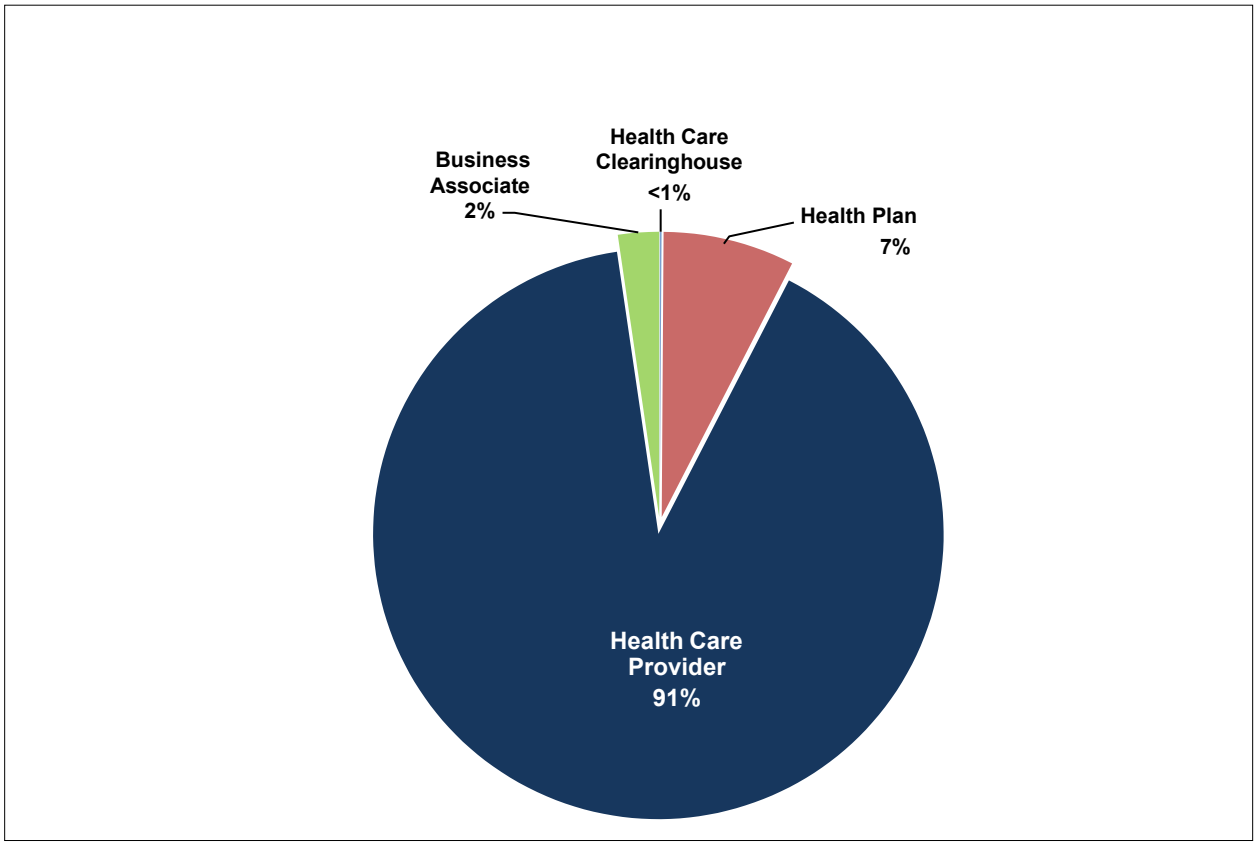

Figure 7

HHS Office for Civil Rights
Breach Reports of Unsecured PHI affecting Fewer Than 500 Individuals in 2021 by Percentage of Individuals Affected by Entity Type

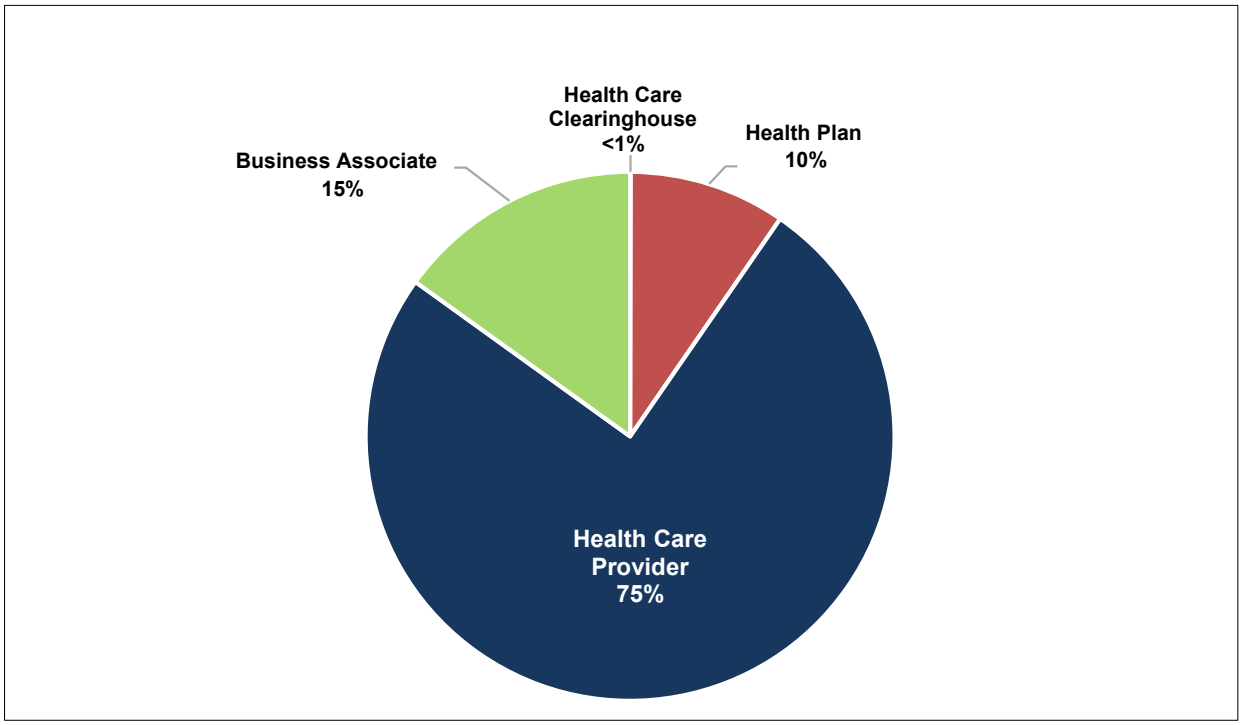

Figure 8

The most common causes or types of breach incidents (in order of frequency) for breaches affecting fewer than 500 individuals were:[20]

(1) Unauthorized access or disclosure (59,811 reports (94%) affecting 208,543 individuals (65%));
(2) Loss (1,989 reports (3%) affecting 10,960 individuals (3%));
(3) Hacking/IT incident (844 reports (1%) affecting 77,469 individuals (24%))
(4) Theft (735 reports (1%) affecting 17,173 individuals (5%)); and
(5) Improper disposal (192 reports (<1%) affecting 5,070 individuals (2%)).

See Figures 9 and 10.

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

HHS Office for Civil Rights
Breach Reports of Unsecured PHI affecting Fewer Than 500 Individuals in 2021 by Percentage of Reports Received by Type of Breach

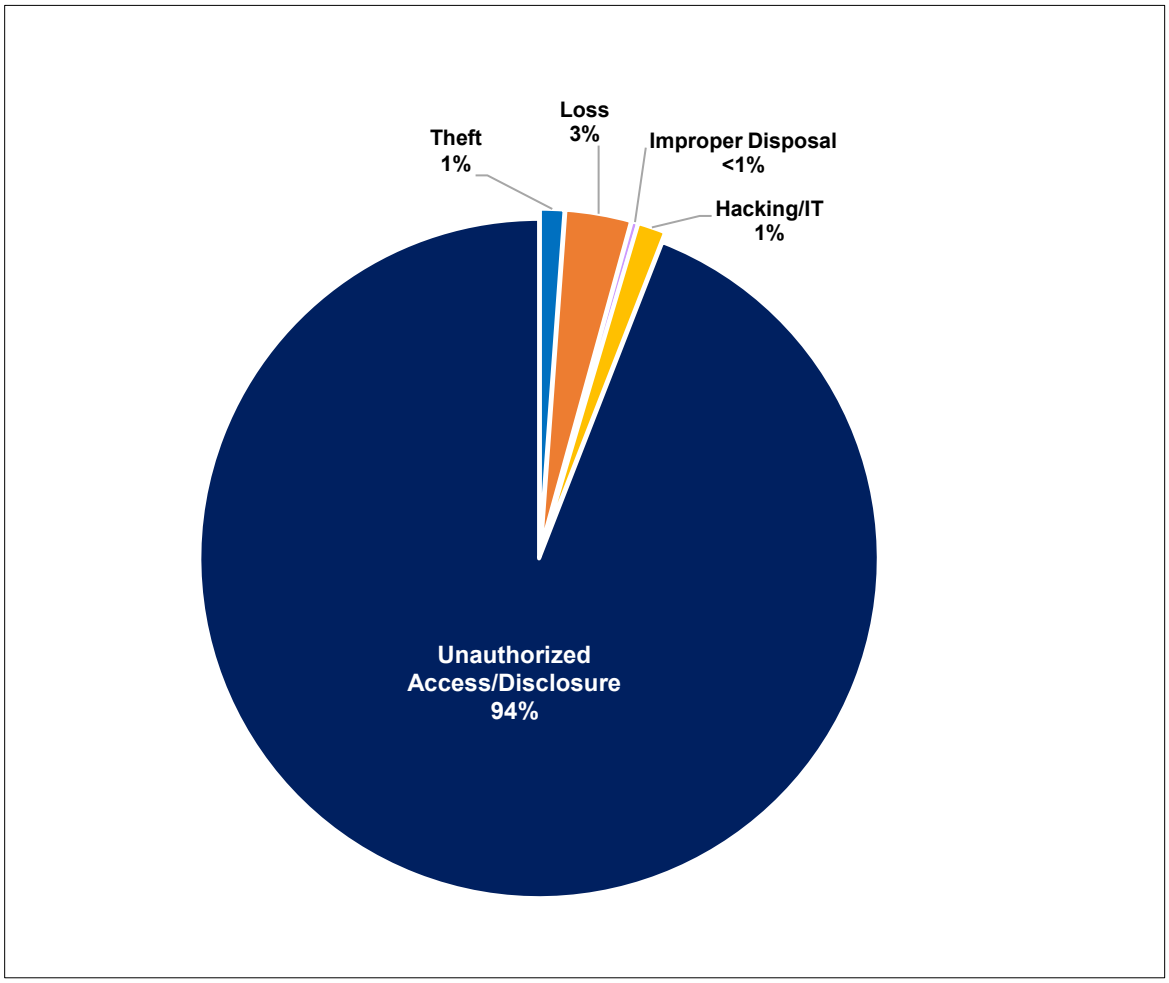

Figure 9

HHS Office for Civil Rights
Breach Reports of Unsecured PHI affecting Fewer Than 500 Individuals in 2021 by Percentage of Individuals Affected by Type of Breach

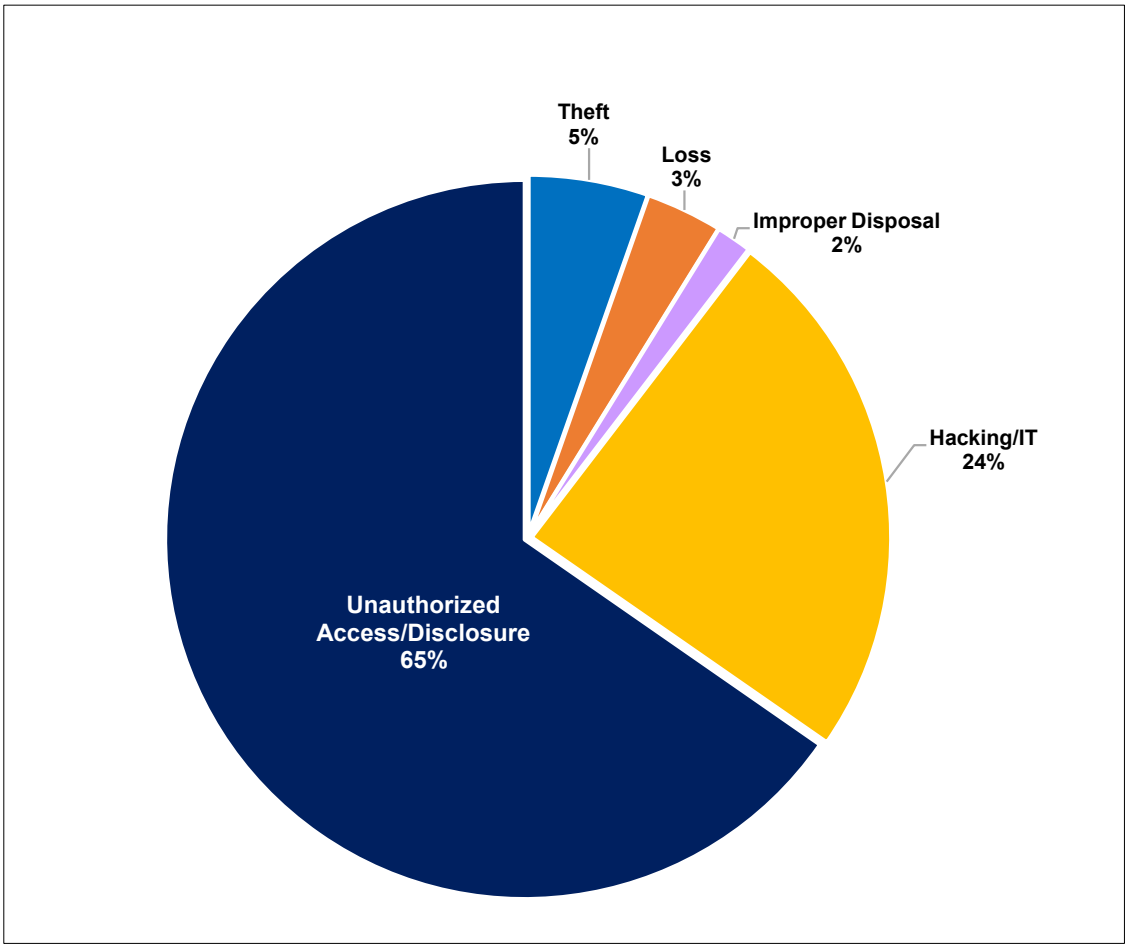

Figure 10

The 63,571 reported breaches affecting fewer than 500 individuals described the following locations of the PHI (in order of frequency):[21]

(1) Paper (44,680 reports (70%) affecting 141,409 individuals (44%));
(2) Electronic medical record (EMR) (7,873 reports (12%) affecting 23,757 individuals (7%));
(3) Other (5,822 reports (9%) affecting 24,068 individuals (8%));[22]
(4) E-mail (3,309 reports (5%) affecting 62,424 individuals (20%));

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

(5) Desktop computer (670 reports (1%) affecting 8,125 individuals (3%));
(6) Network server (548 reports (1%) affecting 49,381 individuals (15%));
(7) Other portable electronic device (528 reports (1%) affecting 4,127 individuals (1%)); and
(8) Laptop computer (141 reports (< 1%) affecting 5,924 individuals (2%)).

See Figures 11 and 12.

HHS Office for Civil Rights
Breach Reports of Unsecured PHI affecting Fewer Than 500 Individuals in 2021 by Percentage of Reports Received by Location of Breach

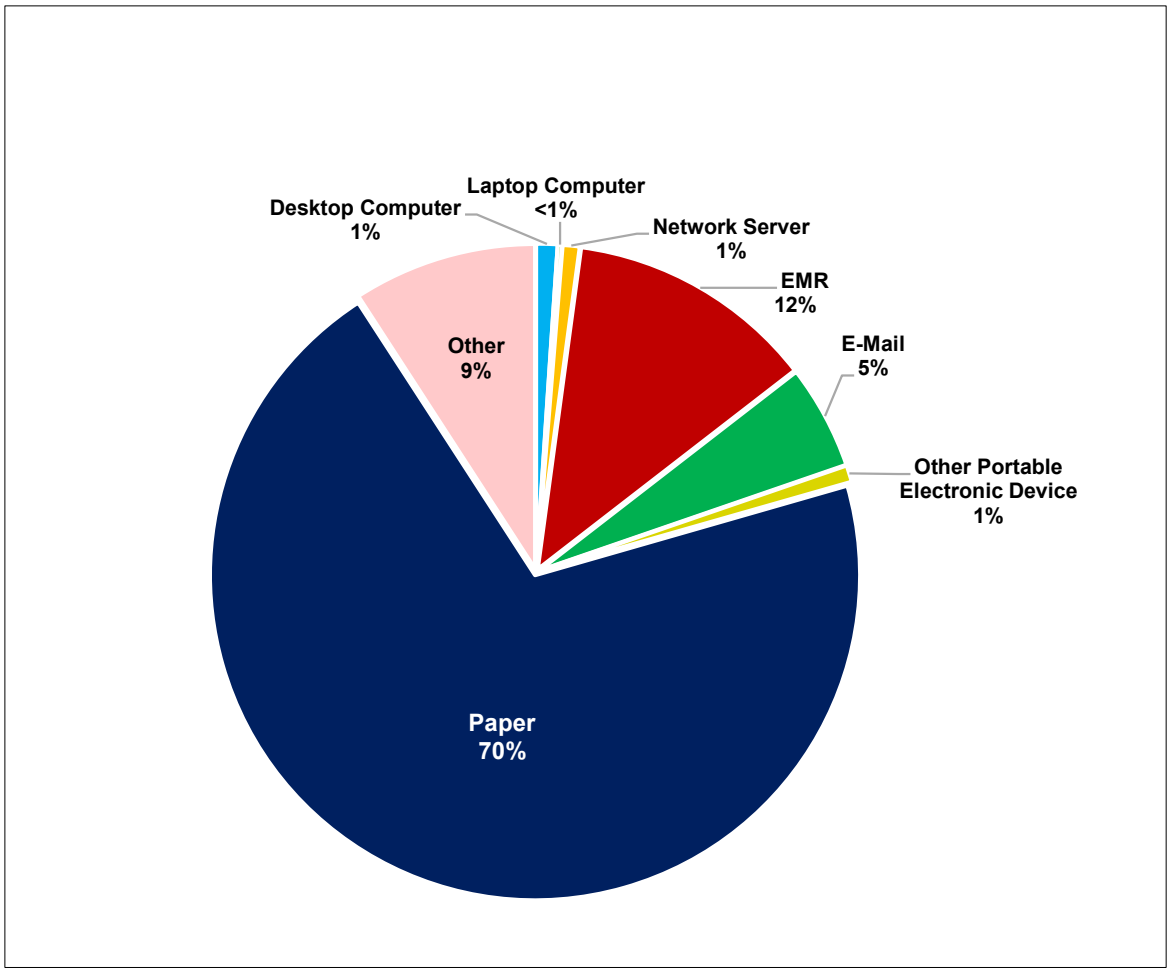

Figure 11

HHS Office for Civil Rights
Breaches of Unsecured PHI affecting Fewer Than 500 Individuals in 2021 by Percentage of Individuals Affected by Location of PHI

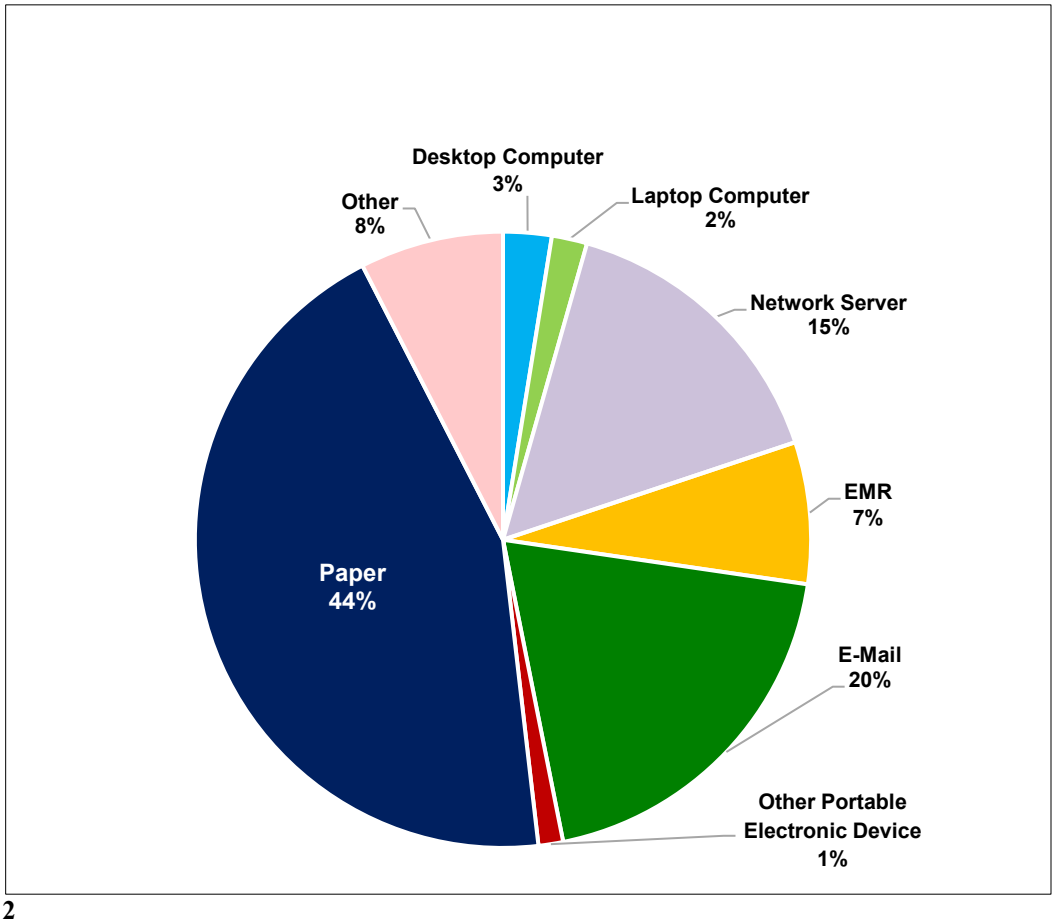

Figure 12

Details on breaches involving fewer than 500 individuals for 2021

As in previous years, breach incidents reported for 2021 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 2021 were due to employees who impermissibly accessed the medical records of co-workers, family, friends, and other individuals without a business need. In response to these incidents, covered entities commonly reported taking remedial actions such as fixing "glitches" in software that incorrectly compiled lists of patient names and contact information, revising policies and procedures,training or retraining employees who handle PHI, and sanctioning employees.

OCR completed 22 breach investigations involving fewer than 500 individuals in 2021.

Cases Investigated and Action Taken

OCR opened investigations into all 609 reported breaches affecting 500 or more individuals that occurred in 2021. OCR also opened 22 investigations into breaches affecting fewer than 500 individuals. OCR completed 554 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 thatwere resolved in 2021 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 2021.

Lessons Learned

The breach reports submitted to OCR offer insight into common areas of vulnerability in protections for the privacy and security of individuals' PHI. Covered entities and business associates should consider the following HIPAA Security Rule standards and implementation specifications that were identified in OCR investigations in 2021 as areas needing improvement.

- Security Management Process Standard. The Security Rule requires regulated entities to implement policies and procedures to prevent, detect, contain, and correct security violations. Specific implementation specifications within this administrative safeguard standard needing improvement include:

    - Risk Analysis. 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 covered entity or business associate. Failures to conduct a risk analysis leave regulated entities vulnerable to breaches of unsecured ePHI as cybersecurity attacks are increasing.

    - Risk Management. 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. Failures to implement risk management leave regulated entities vulnerable to breaches of unsecured ePHI as cybersecurity attacks are increasing.

    - Information System Activity Review. 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 found instances of deficient or non-existent information system activity review processes. Examples of deficient processes include a total lack of review of information system activity as well as reviews that were ad hoc and reactive. A successful system activity review process can play a critical role in detecting malicious activity, including from malicious insiders. Early detection of

malicious activity can be key to eliminating or mitigating potential breaches and reducing the potential number of individuals affected.

- Audit Controls Standard. 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 can be used not only to detect malicious activity, but also to enable review of malicious activity that may have previously occurred. OCR's investigations continued to find regulated entities that either do not have such mechanisms in place or have implemented audit control mechanisms for only a narrow subset of its systems containing or using ePHI. 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.

- Access Control Standard. The Security Rule requires regulated entities to implement technical policies and procedures for electronic information systems that maintain ePHI to allow access to only those persons or software programs that have been granted access rights in accordance with a regulated entity's information access management policies and procedures. OCR's investigations found evidence of non-compliance with the access control standard, which was often a contributing factor to a breach of ePHI. Examples of ineffective access controls OCR discovered led to escalation of privileges, unimpeded lateral movement to systems and networks within an organization, and deployment of malicious software. Effective access controls can prevent breaches of ePHI or reduce the number of individuals affected.

Summary and Conclusion

The number of breaches experienced by regulated entities continue to rise and hacking/IT incidents remain the largest category of breaches of unsecured PHI occurring in 2021 affecting 500 or more individuals, at 75% of the reports received and 95% of the individuals affected. Health care providers experienced the majority of these (72%), which affected over 24.3 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 2021, unauthorized access or disclosure was the largest category of type of breach reported (94%), and paper records was the largest by location (70%).

The breach notifications requirements increase public transparency of breaches within the regulated industry and the 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. To provide increased public transparency, information about breaches involving 500 or more individuals is available for public view on the OCR website at www.hhs.gov/hipaa/for-professionals/breach-notification/index.html. The breaches are posted in an accessible format that allows users to search and sort the posted breaches by name of covered entity, name of business associate (if applicable), state, number of individuals affected, date of breach, type of breach, and location of the breached information (e.g., laptop computer). Additionally, the website provides brief summaries of the enforcement cases, including breach report investigations that OCR has investigated and closed.

OCR continues to exercise its oversight responsibilities by reviewing and responding to breach notification reports and initiating investigations into all breaches affecting 500 or more individuals, as well as into select breaches affecting fewer than 500 individuals. During 2021, OCR resolved two breach investigations with resolution agreements/corrective action plans and collected settlements totaling over $5.1 million.[23]

[23] The two cases were Excellus Health Plan and Peachstate Health Management dba AEON Clinical Laboratories.

APPENDIX

Resolution Agreements[24] in 2021

Resolution Agreement with Excellus Health Plan

Excellus Health Plan (Excellus) agreed to pay $5,100,000 and to implement a corrective action plan to settle potential violations of the HIPAA Privacy and Security Rules. Excellus is a New York health services corporation that provides health insurance coverage in Upstate and Western New York.

OCR began investigating Excellus after it filed a breach report stating that cyber-attackers had gained unauthorized access to its information technology systems. The hackers installed malware and conducted reconnaissance activities that ultimately resulted in the impermissible disclosure of the PHI of more than 9.3 million individuals. OCR's investigation found potential violations of the HIPAA Rules including failure to conduct an accurate and thorough risk analysis and failures to implement risk management, information system activity review, and access controls.

In addition to the monetary settlement, Excellus agreed to:

- Complete a comprehensive and thorough risk analysis;
- Develop an enterprise-wide Risk Management Plan to address and mitigate any security risks and vulnerabilities found in the risk analysis; and
- Revise or develop policies and procedures to comply with the HIPAA Rules.

This settlement occurred in January 2021. The resolution agreement is available at the following link:
www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/excellus/index.html.

Resolution Agreement with Peachstate Health Management dba AEON Clinical Laboratories

Peachstate Health Management dba AEON Clinical Laboratories (Peachstate), agreed to pay $25,000 and to implement a corrective action plan to settle potential violations of the HIPAA Security Rule. Peachstate is based in Georgia and provides diagnostic and laboratory-developed tests, including clinical and genetic testing services.

In December 2017, OCR initiated a compliance review of Peachstate to determine its compliance with the HIPAA Privacy and Security Rules. OCR's investigation found indicia of systemic noncompliance with the HIPAA Security Rule, including failures to conduct a comprehensive and thorough risk analysis, implement risk management and audit controls, and maintain documentation of HIPAA Security Rule policies and procedures.

In addition to the monetary settlement, Peachstate agreed to:

[24] 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 2021.

- Complete a comprehensive, enterprise-wide risk analysis;
- Develop a Risk Management Plan to address and mitigate any security risks and vulnerabilities found in the risk analysis;
- Develop and distribute policies and procedures to comply with the HIPAA Rules; and
- Train all workforce members who have access to PHI on the HIPAA policies and procedures.

This settlement occurred in April 2021. The resolution agreement is available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/peachstate/index.html.