United States Government Accountability Office

Report to Congressional Committees

May 2022

ELECTRONIC HEALTH INFORMATION

HHS Needs to Improve Communications for Breach Reporting

Accessible Version

GAO-22-105425

GAO Highlights

Highlights of GAO-22-105425, a report to congressional committees

Why GAO Did This Study

The use of IT allows health care providers and others to share health care information electronically, which enhances care delivery, public health and research; and empowers providers to make informed decisions regarding patient health.

HHS sets and enforces standards for protecting electronic health information. To implement the provisions of HIPAA, HHS issued regulations that govern PHI transmitted or maintained by covered entities, such as health plans and health care providers, and their business associates.

GAO was asked to review covered entities' required reporting to HHS on data breaches. This report examines (1) the number of breaches and affected individuals reported to HHS since 2015; (2) the extent to which HHS established a review process to assess whether covered entities had implemented recognized security practices; and (3) the extent to which improvements can be made related to HHS's breach reporting requirements.

To do so, GAO reviewed privacy and information security laws; analyzed HHS documentation, policies, and procedures; and interviewed cognizant OCR officials. GAO also surveyed HIPAA covered entities and business associates.

What GAO Recommends

GAO is making one recommendation to HHS to establish a feedback mechanism to improve the effectiveness of its breach reporting process. HHS concurred with GAO's recommendation and described actions it would take to address it.

View GAO-22-105425. For more information, contact Jennifer R. Franks at (404) 679-1831 or FranksJ@gao.gov or Marisol Cruz Cain at (202) 512-5017 or CruzCainM@gao.gov.

May 2022

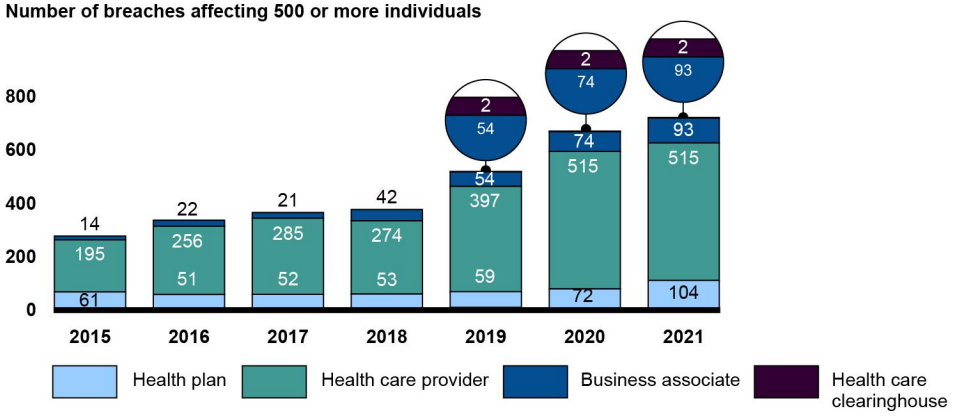
ELECTRONIC HEALTH INFORMATION

HHS Needs to Improve Communications for Breach Reporting

What GAO Found

Since 2015, the Department of Health and Human Services (HHS) has seen an increase in reported breaches while the number of affected individuals has varied each year from approximately 5 to 113 million. Such breaches of health information involve the unauthorized (intentional or unintentional) exposure, disclosure, or loss of an individual's identifiable health information. The figure shows the number of breaches reported by various covered entities from 2015 through 2021.

Figure: The Number of Breaches Involving Unsecured Protected Health Information (PHI) from 2015 to 2021



Source: GAO analysis of Department of Health and Human Services' January 2022 data. | GAO-22-105425

*Note: Business associates are entities that perform certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a covered entity. Health care clearinghouses are entities that process nonstandard data elements of health information they receive from another entity into standard data elements or vice versa.

The HHS Office for Civil Rights (OCR), the unit responsible for enforcing the Health Insurance Portability and Accountability Act (HIPAA) standards, has taken steps to establish a process on whether entities implemented recognized security practices. A law enacted in January 2021 required HHS, as part of its enforcement activities, to consider whether covered entities had implemented such practices. In response, OCR established standard operating procedures for its investigators, published a request for information to seek public comments on implementation of security practices, and is conducting outreach to the health care sector. OCR expects to finalize the process no later than the summer of 2022.

OCR is charged with implementing and enforcing the HIPAA Privacy, Security and Breach Notification Rules, including the development and management of the breach reporting process. However, OCR does not have a method for covered entities to provide feedback on the breach reporting process, nor did the office indicate that it had plans to develop one. Without a clear mechanism to provide feedback to OCR, covered entities and business associates can face challenges during the breach reporting process. Further, soliciting feedback on the breach reporting process could help OCR improve aspects of the process.

Contents

Letter 1

Background 5
Breaches Reported to HHS Have Steadily Increased since 2015, but the Number of Affected Individuals Has Varied 16
HHS Is Taking Steps to Establish a Process to Review Recognized Security Practices during Investigations 23
OCR Lacks a Mechanism for Soliciting Feedback from Covered Entities on Its Processes 25
Conclusions 27
Recommendation for Executive Action 28
Agency Comments 28

Appendix I: Objectives, Scope, and Methodology 30

Appendix II: Comments from the Department of Health and Human Services 32

Agency Comment Letter 34

Appendix III: GAO Contacts and Staff Acknowledgments 36

Staff Acknowledgments 36

Table

Table 1: Common Cyber Threat Actors to the Healthcare and Public Health Sector 14

Figures

Figure 1: Examples of Covered Entities and Business Associates Required to Report Breaches to the Department of Health and Human Services 9
Figure 2: The Office for Civil Rights' Breach Investigation Process for Breaches Involving 500 or More Individuals 11
Figure 3: Number of Breaches Involving Unsecured Protected Health Information from 2015 to 2021 17
Figure 4: Number of Breaches Involving Unsecured Protected Health Information Reported by Covered Entities and Business Associates by Breach Type from 2015 to 2021 19
Figure 5: Number of Breaches Involving Unsecured Protected Health Information by Breach Type from 2015 to 2021 20

Figure 6: Number of Individuals Affected by Breaches Involving Unsecured Protected Health Information from 2015 to 2021 22

Abbreviations

EHR	electronic health record
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
HITECH Act	Health Information Technology for Economic and Clinical Health Act
National Plan	National Infrastructure Protection Plan
OCR	Office for Civil Rights
PHI	protected health information
PII	personally identifiable information
Privacy Rule	Standards for Privacy of Individually Identifiable Health Information
Security Rule	Security Standards for the Protection of Electronic Protected Health Information

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

May 27, 2022

The Honorable Ron Wyden
Chairman
The Honorable Mike Crapo
Ranking Member
Committee on Finance
United States Senate

The Honorable Patty Murray
Chair
The Honorable Richard Burr
Ranking Member
Committee on Health, Education, Labor, and Pensions
United States Senate

The health care sector uses a vast array of information systems and technologies across multiple settings, such as physician offices and hospitals. The use of IT, including electronic health records (EHR) systems, has allowed health care providers and others to share health care information electronically. Specifically, interoperable health IT systems enable multiple health IT systems to access, exchange, and use all electronically accessible health information.[1] This interoperable exchange allows health care providers and patients to securely find and use vital health information. This, in turn, enhances care delivery, public health, and research; and empowers providers to make informed decisions regarding patient health.

While EHR and interoperable health IT offer many benefits, they are also susceptible to breaches.[2] We previously reported on the trends in these breaches from 2009 to 2015, which found that there were over 113 million

[1]Interoperability, with respect to health IT, means technology that enables the secure exchange and use of electronic health information with, and from, other health IT without special effort on the part of the user.

[2]A breach is an unauthorized or unintentional exposure, disclosure, or loss of an organization's sensitive information.

records that were breached in 2015.[3] According to the 2021 Mandiant M Trends Report, the health care industry remains one of the three most targeted industries by cyberattacks since 2016.[4] The recent trends of breaches in the health care sector have highlighted the importance of ensuring the security and privacy of electronic health information, including such information maintained in EHRs. Two laws, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH Act), provide for the creation, enforcement, and monitoring of information security and privacy standards for electronic health data.[5] Under these two laws, the Department of Health and Human Services (HHS) has primary responsibility for setting and enforcing standards governing protected health information (PHI), including electronic PHI.[6] HHS has delegated this HIPAA enforcement function to the Office for Civil Rights (OCR). HHS has issued regulations to implement HIPAA, which

[3]GAO, *Electronic Health Information: HHS Needs to Strengthen Security and Privacy Guidance and Oversight*, GAO-16-771 (Washington, D.C.: Aug. 26, 2016).

[4]FireEye Mandiant, *M-Trends 2021,* (Milpitas, CA:2021).

[5]Pub. L. No. 111-5, Div. A, Title XIII, 123 Stat. 115, 226-279 and Div. B, Title IV, 123 Stat. 467-496 (Feb. 17, 2009); and Pub. L. No. 104-191, Title II, Subtitle F, 110 Stat. 1936, 2021 (Aug. 21, 1996) (codified at 42 U.S.C. §§ 1320d–1320d-9).

[6]PHI is defined as individually identifiable health information transmitted or maintained by a covered entity or its business associate in any form or medium (45 C.F.R § 160.103). The definition exempts a small number of categories of individually identifiable health information, such as information found in employment records held by a covered entity in its role as an employer. Individually identifiable health information includes demographic data collected from an individual, that (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; (2) relates to the past, present, or future physical or mental health or condition of the individual or the provision of or payment for health care to the individual; and (3) can be used to identify the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

among other things, requires covered entities and their business associates to notify HHS of breaches of unsecured PHI.[7]

You asked us to conduct a study on breaches reported by covered entities to HHS. Accordingly, this report examines:

1. the number of breaches and affected individuals covered entities have reported to HHS since 2015;
2. the extent to which HHS established a review process to assess whether covered entities had implemented recognized security practices; and
3. the extent to which improvements can be made related to HHS's breach reporting requirements.

To address the first objective, we analyzed prior GAO reports that identified security, as well as, privacy threats to electronic heath data and information systems.[8] Further, we analyzed information provided by HHS on the number of breaches affecting 500 or more individuals and interviewed cognizant HHS officials about the data.[9] We assessed the reliability of the breach data by assessing the sufficiency and appropriateness of the computer-processed data. Specifically, we reviewed written responses to our data reliability questions from knowledgeable HHS officials to clarify any issues. In addition, to verify

[7]Covered entities are required by 45 C.F.R. § 164.408 to notify HHS of breaches of unsecured PHI. HIPAA covered entities are health plans, health care providers who transmit any health information in electronic form in connection with certain financial or administrative transactions, and health care clearinghouses. Health care clearinghouses process nonstandard data elements of health information they receive from another entity into standard data elements or vice versa. Business associates create, receive, maintain, or transmit protected health information on behalf of a covered entity or another business associate; or provide certain services to or for a covered entity where the provision of the service involves the disclosure of protected health information. 45 C.F.R. § 160.103.

[8]GAO, *Cybersecurity: HHS Defined Roles and Responsibilities, but Can Further Improve Collaboration,* GAO-21-403 (Washington, D.C.; June. 28, 2021); GAO-16-771; *Electronic Health Records: HHS Strategy to Address Information Exchange Challenges Lacks Specific Prioritized Actions and Milestones*, GAO-14-242 (Washington, D.C.: Mar. 24, 2014).

[9]According to the Health Insurance Portability and Accountability Act (HIPAA) of 1996, as amended by the HITECH Act of 2009, a covered entity must notify HHS of a breach that affected more than 500 individuals within 60 calendar days of discovery and OCR investigates each these breaches. For breaches that affect less than 500 individuals, the reporting requirement changes to 60 days after the end of each calendar year and investigations are initiated at HHS's discretion.

that the data did not include obvious errors such as missing data fields or unexplained outliers, our analysis was confirmed by a second, independent analyst on the engagement team in consultation with the team's methodologist. Through these steps, we determined that the data were sufficiently reliable for our purposes.

To address the second objective, we reviewed relevant information security and privacy laws, including HIPAA and HITECH Act, as amended, and the implementing regulations.[10] We identified requirements in the law governing HHS's responsibilities to consider whether covered entities or business associates implemented recognized security practices. We also interviewed knowledgeable OCR officials to identify any existing processes that relate to considering recognized security practices during an investigation.

To address the third objective, we compared OCR's breach reporting and investigation process against leading practices to determine the extent to which OCR's processes aligned. We also interviewed HHS officials to gain a better understanding of their processes and any relevant efforts under way that could address identified flaws. Lastly, we developed a non-generalizable survey to gather the opinions of covered entities and business associates on OCR's breach reporting requirements and breach investigations. The Health Information Sharing and Analysis Center, Healthcare and Public Health Sector Coordinating Council, and the American Hospital Association distributed the survey questions to over 48,000 of their members.[11] While the results of the survey cannot be generalized, they allowed us to learn, in detail, about the actual experiences of many different types of covered entities and business associates. See Appendix I for a more detailed discussion of our objectives, scope, and methodology.

We conducted this performance audit from September 2021 to May 2022 in accordance with generally accepted government auditing standards.

[10]Pub. L. No. 116-321, 134 Stat. 5072 (Jan. 5, 2021) amends the HITECH Act and adds section 13412 that sets out requirements regarding the recognition of security practices.

[11]The Health Information Sharing and Analysis Center distributed the survey to approximately 5,000 individuals from 700 firms globally. The Healthcare and Public Health Sector Coordinating Council distributed the survey to approximately 660 individuals from 332 organizations, and the American Hospital Association distributed the survey to approximately 43,000 individuals from approximately 5,000 health care organizations. We conducted the survey from January 31, 2022 until February 11, 2022 and received a total of 141 complete responses from covered entities and business associates from various health subsectors and various organizational sizes and roles.

Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Electronically exchanging information is important in health care delivery. One key example is an EHR—a digital version of a patient's paper medical record or chart that makes information available to authorized users. EHRs can contain sensitive data such as a patient's medical and treatment history, diagnoses, medications, treatment plans, immunization dates, allergies, radiology images, and laboratory and test results. These records can also give a provider access to evidence-based tools for making decisions about a patient's care and can automate certain workflows.

System software for managing EHRs is typically purchased by providers (such as physicians, hospitals, and health systems) from vendors that develop the systems. When these systems are interoperable, information can be exchanged—sent from one provider to another—and then integrated into the receiving provider's EHR system, allowing the provider to use that health information to inform clinical care.

HIPAA Requires HHS to Develop and Enforce Security and Privacy Standards

HIPAA authorized the Secretary of HHS to establish standards to protect the privacy of certain health information and required the Secretary to adopt security standards for that health information.[12] HHS implemented the HIPAA provisions, as amended by the HITECH Act, through its issuance of the Privacy, Security, Enforcement, and Breach Notification Rules. The Rules are collectively known as the HIPAA Rules, which

[12]Pub. L. No. 104-191, Title II, Subtitle F, 110 Stat. 1936, 2021 (Aug. 21, 1996) (codified at 42 U.S.C. §§ 1320d–1320d-9).

govern PHI transmitted or maintained by covered entities and their business associates.[13] The HIPAA Rules are described below.

- The Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) establishes national standards for safeguarding PHI, which includes most individually identifiable health information transmitted or maintained in any form by a covered entity or its business associates.[14] The Privacy Rule generally prohibits the use or disclosure of PHI except in the circumstances set out in the regulations and provides individuals with privacy rights with regard to their health information. For example, the Privacy Rule provides individuals with the right to request restrictions on uses and disclosures of PHI, the right to adequate notification of privacy practices, the right of access to PHI, and the right to request amendments to inaccurate or incomplete PHI. In addition, the Privacy Rule requires that a covered entity or business associate employ appropriate safeguards and, in most cases, make reasonable efforts to use, disclose, or request only the minimum necessary PHI to accomplish the intended purpose.
- The Security Standards for the Protection of Electronic Protected Health Information (Security Rule) establishes nationwide standards for safeguarding PHI that is held or transferred electronically, or electronic PHI.[15] It operationalizes the protections contained in the

[13]HIPAA covered entities are health plans, health care providers, and health care clearinghouses. Health care clearinghouses process nonstandard data elements of health information they receive from another entity into standard data elements or vice versa. Business associates generally create, receive, maintain, or transmit PHI on behalf of a covered entity or another business associate for a "covered function", or provide certain services to or for such covered entity, where the provision of the services to or for such covered entity includes the disclosure of PHI. 45 C.F.R. §§ 160.103. Pub. L. No. 111-5, Div. A, Title XIII, 123 Stat. 115, 226-279 and Div. B, Title IV, 123 Stat. 467-496 (Feb. 17, 2009). The HIPAA Privacy, Security, Enforcement, and Breach Notification Rules were issued at 45 C.F.R. Parts 160 and 164 and were updated at 78 Fed. Reg. 5566 (Jan. 25, 2013) and 79 Fed. Reg. 7290 (Feb. 6, 2014).

[14]Individually identifiable health information includes demographic data collected from an individual, that (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; (2) relates to the past, present, or future physical or mental health or condition of the individual or the provision of or payment for health care to the individual; and (3) can be used to identify the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. 45 C.F.R. § 160.103.

[15]Protected health information that a covered entity or business associate maintains or transmits in electronic form is referred to as electronic protected health information, a subset of information covered by the Privacy Rule. 45 C.F.R. 160.103

Privacy Rule by specifying administrative, physical, and technical safeguards to secure individuals' electronic PHI. For example, the Security Rule requires organizations to complete a risk analysis that is an accurate and thorough assessment of the potential risks and vulnerabilities to the electronic PHI held by the covered entity or business associate. The Security Rule also requires covered entities and business associates to implement risk management practices such as implementing sufficient security measures to reduce potential risks and vulnerabilities to a reasonable and appropriate level.

- The Enforcement Rule sets out requirements and procedures governing HHS's investigatory authority and the ability to impose civil money penalties on covered entities and business associates, where applicable. The Secretary of HHS delegated these responsibilities to OCR, which is charged with implementing and enforcing the HIPAA Rules.
- The Breach Notification Rule requires covered entities to notify HHS of breaches of unsecured PHI.[16] In addition, the HITECH Act requires business associates to notify the covered entity without unreasonable delay and no later than 60 days from the discovery of the breach. To comply with this breach notification requirement, covered entities notify HHS of breaches through a reporting system on HHS's breach portal. For breaches that affected 500 or more individuals, covered entities must submit a notification to HHS within 60 days after the discovery of a breach. For breaches affecting fewer than 500 individuals, covered entities must notify HHS within 60 days after the end of the calendar year in which the breach occurred.

The HITECH Act, enacted in 2009, amended HIPAA and strengthened the privacy and security protections for health information established by HIPAA and the HIPAA Rules by:

- extending the applicability of specific Privacy and Security Rules' requirements to the business associates of covered entities;
- requiring HIPAA covered entities and business associates to provide for notification of breaches of unsecured PHI;
- expanding individuals' rights to access their PHI; and

[16]In the HIPAA Rules context, a "breach" is the acquisition, access, use, or disclosure of protected health information in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of that information. 45 C.F.R. § 164.402.

- requiring periodic audits to ensure compliance with the Privacy and Security Rules.

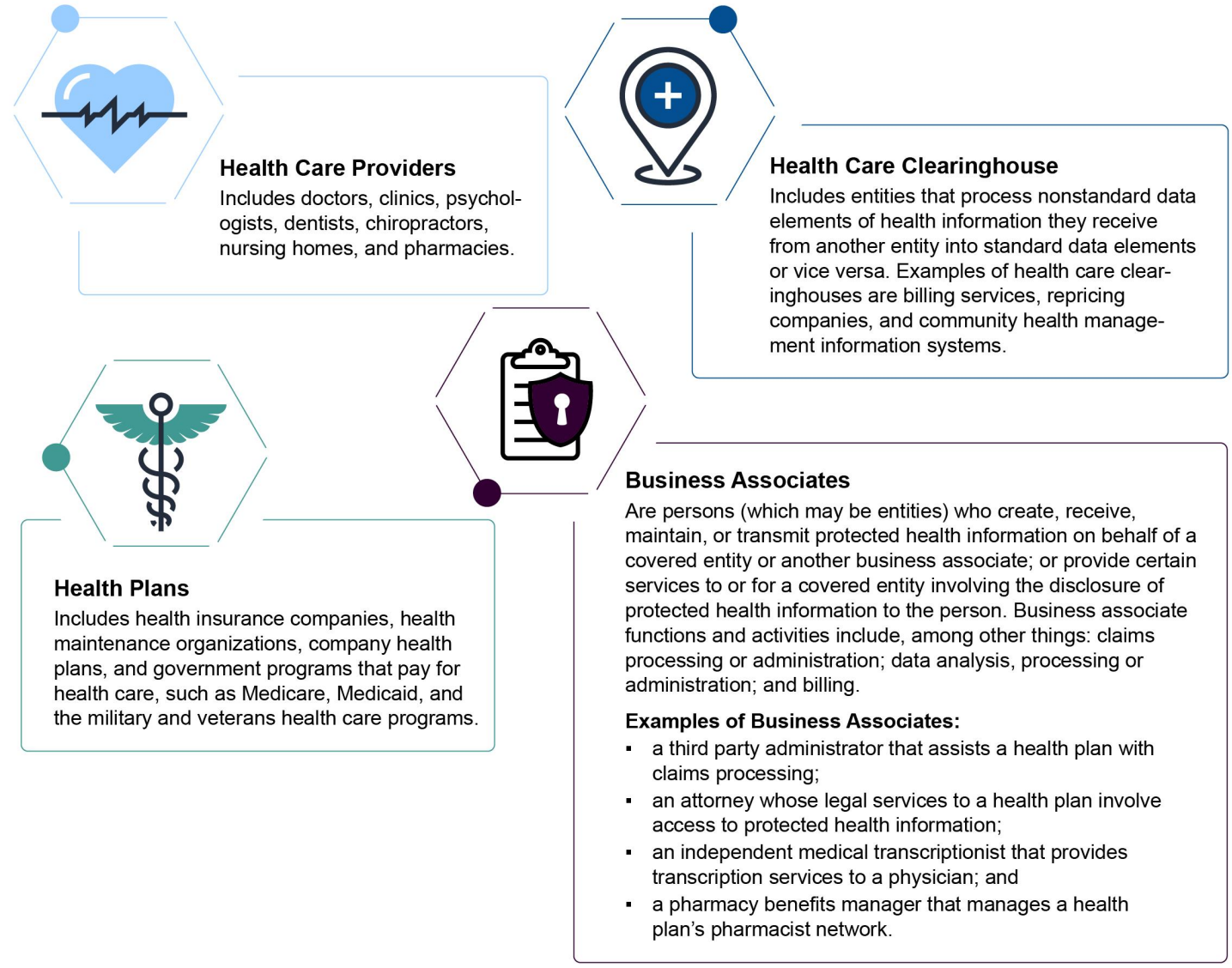
OCR Established a Process for Covered Entities to Report Breaches

One of OCR's roles is to enforce the HIPAA Privacy, Security, and Breach Notification Rules. The office is divided into eight separate regions and a headquarters office in Washington, D.C.[17] To fulfill its HIPAA enforcement responsibilities, OCR has established a process for covered entities to report breaches and a process to initiate investigations of breaches.[18] See Figure 1 for a summary of the various types of covered entities and business associates required to report breaches.

[17]Headquartered in Washington, D.C., the OCR's eight regional offices are located in Boston, Massachusetts (New England Region), New York, New York (Eastern and Caribbean Region), Philadelphia, Pennsylvania (Mid-Atlantic Region), Atlanta, Georgia (Southeast Region), Chicago, Illinois and Kansas City, Missouri (Midwest Region), Dallas, Texas (Southwest Region), Denver, Colorado (Rocky Mountain Region), and San Francisco, California (Pacific Region).

[18]Business associates are not required to report breaches directly to HHS. 45 CFR 164.410. However, an agreement between the covered entity and business associate may specify that the business associate provide notice to HHS on behalf of the covered entity.

Figure 1: Examples of Covered Entities and Business Associates Required to Report Breaches to the Department of Health and Human Services

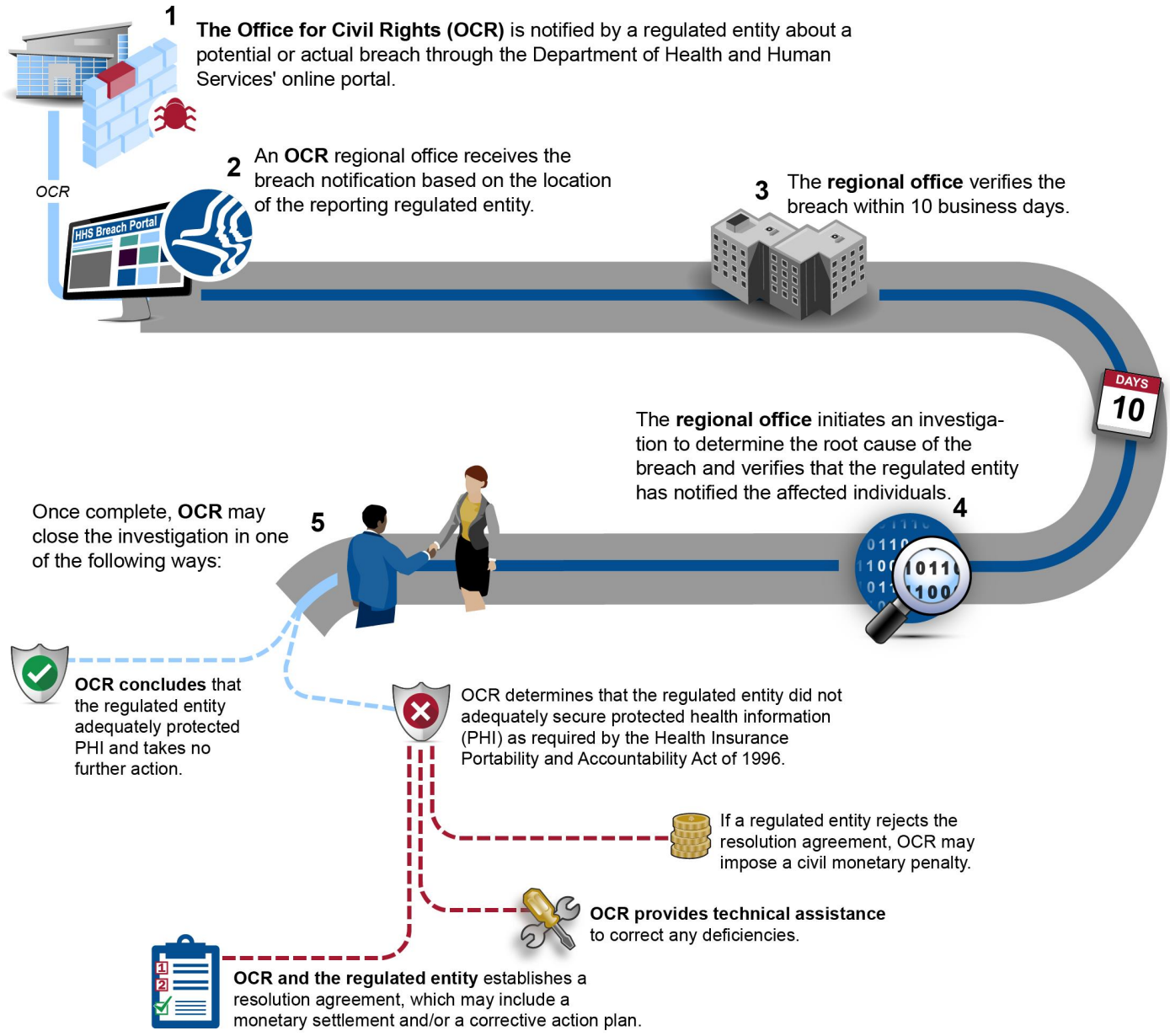


Source: www.hhs.gov and 65 Fed. Reg. 82477 (Dec. 28, 2000); images: vasabii/stock.adobe.com. | GAO-22-105425

Covered entities and business associates, along with members of the public, can submit breach notifications or notifications of other potential violations of the HIPAA Rules through HHS's website, which may prompt an investigation.[19] Alternatively, OCR can initiate its own investigations based on factors such as media reports, patterns of repeat violations, or referrals from other government organizations, among other instigating events. Once OCR receives a breach report involving the PHI of 500 or more individuals, the report is forwarded to the appropriate regional office for further review. See Figure 2 for OCR's breach investigation process for breaches that affected 500 or more individuals.

[19]OCR automatically begins investigations on all breaches affecting 500 or more individuals and initiates investigations on breaches of fewer than 500 individuals at its discretion.

Figure 2: The Office for Civil Rights' Breach Investigation Process for Breaches Involving 500 or More Individuals



Source: GAO analysis of OCR's data breach investigations process. | GAO-22-105425

*Note: The term "regulated entity" includes both covered entities and business associates.

Once the investigation is complete, there are multiple ways that OCR can conclude the investigation. For example:

- If no potential violations of the HIPPA Rules are identified, OCR closes the investigation and takes no further action.
- If potential violations of the HIPPA Rules are identified, OCR could:
  - provide the covered entity or business associate with technical assistance, such as addressing any deficiencies in policies and procedures and privacy practices;
  - request that the covered entity or business associate implement relevant corrective actions and close the investigation upon verifying the actions have been fully implemented;
  - send the case to enforcement and initiate a resolution agreement that typically lasts about three years. Specifically, the agreement may include a resolution amount payment and/or a corrective action plan if violations were discovered.[20] As part of the agreement, the covered entity or business associate must periodically report its progress to OCR regarding correcting any deficiencies identified in the corrective action plan. OCR may also provide technical assistance as part of the agreement during this monitoring period; or
  - impose a civil monetary penalty if covered entities and business associates choose the penalty in lieu of entering into a resolution agreement that requires the implementation of corrective actions or an informal agreement.[21]

Health Care Sector Faces Cybersecurity Challenges

Our nation's critical infrastructures consist of systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on the nation's security, economic stability, public health or safety, or any combination of these factors. Critical infrastructure includes, among other things, banking and financing institutions, telecommunications networks, and energy

[20]A corrective action plan may include steps such as drafting or updating security policies and procedures and implementing access controls. A "resolution amount" is payment included in the resolution agreement that a covered entity or business associate agrees to pay HHS.

[21]The Deputy Director for Health Information Privacy at OCR stated that the imposition of civil monetary penalties at the end of the investigative process is rare and that there has been only seven cases since the beginning of OCR's enforcement program.

production and transmission facilities, most of which are owned and operated by the private sector.

Under federal policy, critical infrastructure is grouped into 16 sectors whose assets, systems, and networks, are considered vital to the security, economy, and/or public health and safety of the United States. These 16 critical infrastructure sectors are chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation; and water and wastewater.

Presidential Policy Directive 21: *Critical Infrastructure Security and Resilience* advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. Among other things, this policy directive states that the federal government shall work with critical infrastructure owners and operators and state, local, tribal, and territorial entities to take proactive steps to manage risk and strengthen the security and resilience of the nation's critical infrastructure. These efforts seek to reduce vulnerabilities, minimize consequences, identify and disrupt threats, and hasten response and recovery efforts related to critical infrastructure. This directive also assigned HHS as the sector risk management agency for the healthcare and public health sector.[22]

Among the key risks facing the nation's critical infrastructures are cybersecurity risks. Specifically, cyber systems supporting federal agencies and our nation's critical infrastructures are inherently at risk. These systems, including health IT systems, are highly complex and dynamic, technologically diverse, and often geographically dispersed. This complexity increases the difficulty in identifying, managing, and protecting the numerous operating systems, applications, and devices comprising the systems and networks. Accordingly, since 1997, we have designated federal information security as a government-wide high-risk area. This area was expanded to include the protecting of critical cyber infrastructure in 2003 and protecting the privacy of personally identifiable information (PII) in 2015.

[22]A sector risk management agency is a federal agency with responsibility for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector.

As previously mentioned, the health care sector uses a vast array of information systems and technologies, with patient care and services provided in multiple settings, such as physician offices and hospitals that are not always well-coordinated. For example, providers may lack real-time access to critical information needed for the care of patients and to ensure that informed decisions are made about the best treatment options because of the lack of coordination.

Moreover, health IT systems can be vulnerable to security lapses, including breaches, that can jeopardize the confidentiality, integrity, and availability of the systems and their information. Cyber threat actors can intrude and use their access to obtain or manipulate sensitive information, such as EHRs, in order to commit fraud or disrupt operations. Further, the loss or unauthorized disclosure of sensitive information, including PHI within EHRs, can lead to serious consequences such as identity theft or other fraudulent activity and can result in substantial harm. Table 1 describes common cyber threat actors that can attack covered entities and business associates.

Table 1: Common Cyber Threat Actors to the Healthcare and Public Health Sector

Threat actor	Description
Criminal Groups	Criminal groups seek to use cyberattacks against health care organizations for monetary gain. Organized criminal groups, which may include organized crime organizations, use spam, phishing, and spyware/malware to commit identity theft, online fraud, and computer extortion.
Hackers	Hackers break into networks for the challenge, revenge, stalking, or monetary gain, among other reasons. Hackers no longer need a great amount of skill to compromise health care systems because they can download commonly available cyberattack tools.
Insiders	Insiders are individuals (e.g., employees, contractors, or vendors) with authorized access to an information system that house electronic health information who have the potential to cause harm, intentionally or unintentionally, through destruction, disclosure, or modification of data, or through denial of service. Insiders could include knowledgeable employees with privileged access to critical health systems or contractors with limited system knowledge.
Nations	Nations, including groups or programs sponsored or sanctioned by nation-states, use cyber tools as part of their information gathering and espionage activities. According to the 2019 *Worldwide Threat Assessment of the U.S. Intelligence Community* and the 2020 *Homeland Threat Assessment*, China and Russia pose the greatest cyberattack threats because they have the ability to launch attacks that could disrupt or damage critical infrastructure, which includes the healthcare and public health sector. While China and Russia are the most capable nation-state cyber adversaries, Iranian and North Korean cyber actors also pose a threat to U.S. systems, networks, and information, according to both assessments.

Source: GAO-21-288 and GAO-21-25. | GAO-22-105425

In a June 2017 report to Congress, the Health Care Industry Cybersecurity Task Force reported that the healthcare and public health sector experienced more breaches than any other critical infrastructure

sector. In addition, the Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation, and HHS issued a joint cybersecurity advisory in October 2020 that reported U.S. hospitals and other health care providers face an increased cybercrime threat, including ransomware attacks and data theft.[23]

Cybersecurity companies in the private sector have also reported about existing cybersecurity risks in the health care *sector.* For example*,* Verizon's *2021 Data* Breach Investigations Report noted that in 2020, cyber actors increased malware attacks, including ransomware, against the healthcare and public health sector. The report also highlighted that the number of ransomware attacks increased, where the cyber threat actors demanded ransom up to multi-million dollars.[24] In addition, IBM's *Cost of a Data Breach Report 2021* highlighted that the health care industry had the highest average cost associated with data breaches for 11 consecutive years.[25] Specifically, health care data breach costs increased from an average total cost of $7.13 million in 2020 to $9.23 million in 2021.

GAO Has Previously Reported on Breaches Involving Electronic Health Information

We previously reported that systems storing and transmitting health information in electronic form are vulnerable to cyber-based threats. The resulting breaches—involving over 113 million records in 2015—had serious adverse impacts such as identity theft, fraud, and disruption of health care services.[26] In addition, we reported that while OCR is charged with implementing and enforcing the HIPAA Rules and has established an enforcement program, OCR had not demonstrated the effectiveness of its program over time.

We made five recommendations specific to HHS's oversight of the breaches involving unsecured PHI to help address these concerns. For example, we recommended HHS update security guidance for covered entities and business associates to ensure that the guidance addresses

[23]Ransomware is a type of malware used to deny access to IT systems or data and hold the systems or data hostage until a ransom is paid.

[24]Verizon, *2021 Data Breach Investigations Report*.

[25]IBM Security, *Cost of a Data Breach Report 2021*.

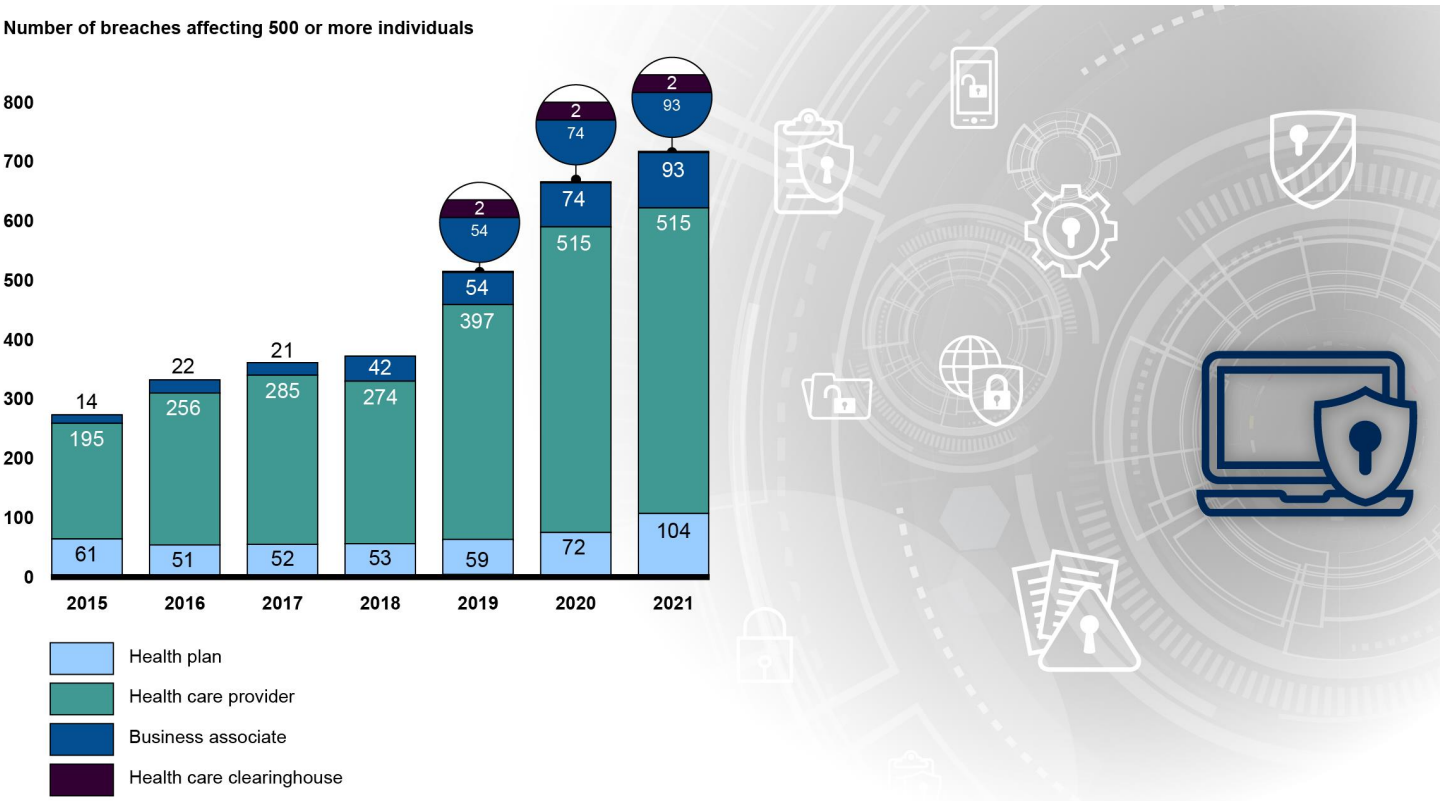
[26]GAO-16-771.

implementation of controls described in the National Institute of Standards and Technology Cybersecurity Framework. HHS has fully implemented these five recommendations.

Breaches Reported to HHS Have Steadily Increased since 2015, but the Number of Affected Individuals Has Varied

According to OCR data, there have been approximately 3,200 total reported breaches from the three types of covered entities (health plans, health care providers, and health care clearinghouses) and their business associates from 2015 to 2021. Of those breaches, health care providers have consistently reported the highest number of breaches compared to other types of covered entities and business associates throughout this timeframe. Figure 3 shows the number of breaches each type of covered entity and business associate reported from 2015 to 2021.

Figure 3: Number of Breaches Involving Unsecured Protected Health Information from 2015 to 2021



Source: GAO analysis of Department of Health and Human Services' January 2022 data; images: bearsky23/stock.adobe.com, Chor muang/stock.adobe.com. | GAO-22-105425

OCR's Deputy Director for Health Information Privacy stated that the number of reported breaches may be correlated with increasing IT-related crimes. According to the Federal Bureau of Investigation, some of the most common IT-related crimes, among others, have included ransomware attacks and business email compromises.[27]

In addition, the Deputy Director said that health care providers may have reported the highest number of breaches because there are significantly more health care providers compared to other types of covered entities. Further, the Deputy Director stated that in general, OCR has observed many instances of covered entities' and business associates' lack of compliance with the Security Rule requirement to conduct accurate and thorough risk analyses. The Deputy added that this may have contributed to the increase in the number of breaches during this time period.[28]

Covered Entities and Business Associates Reported Various Categories of Breaches

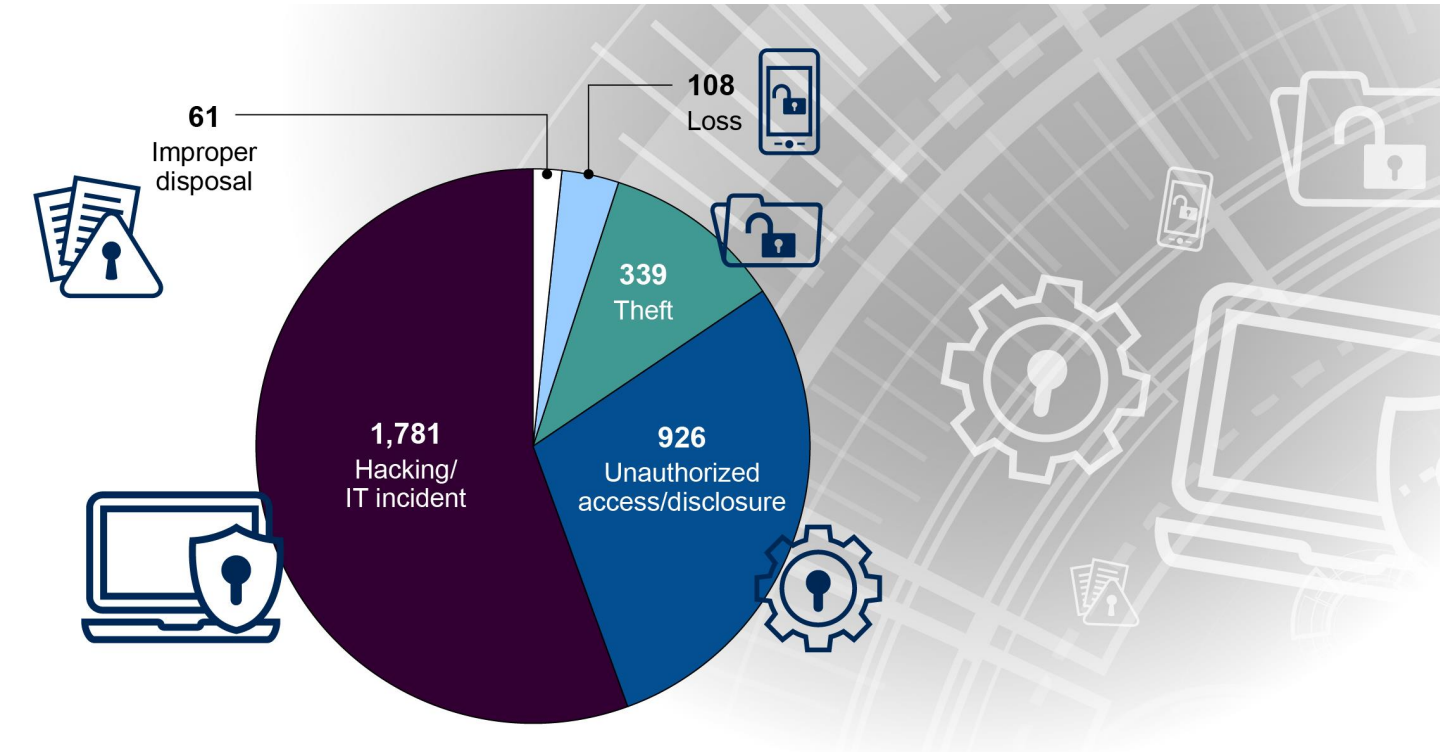
OCR categorizes breaches in the following five categories: hacking and IT incidents, unauthorized access or disclosure, theft, loss, and improper disposal.[29] According to OCR's data, hacking and IT incidents were the most common types of reported breaches overall from 2015 to 2021. Specifically, hacking and IT incidents have accounted for approximately 55 percent of the approximately 3,200 breaches that the covered entities experienced from 2015 to 2021. See Figure 4 for the number of breaches by category from 2015 to 2021.

[27]Business email compromises are sophisticated scams carried out by threat actors compromising email accounts through social engineering (e.g., spoofing of a legitimate known email address) or computer intrusion techniques (e.g., malicious software that can gain access to legitimate email threads about billing/invoices) to conduct unauthorized transfer of funds.

[28]Covered entities and business associates are required to conduct an accurate and thorough analyses of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information that it holds. 45 C.F.R. § 164.308(a)(1).

[29]The National Institute of Standards and Technology defines an IT incident as an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits.

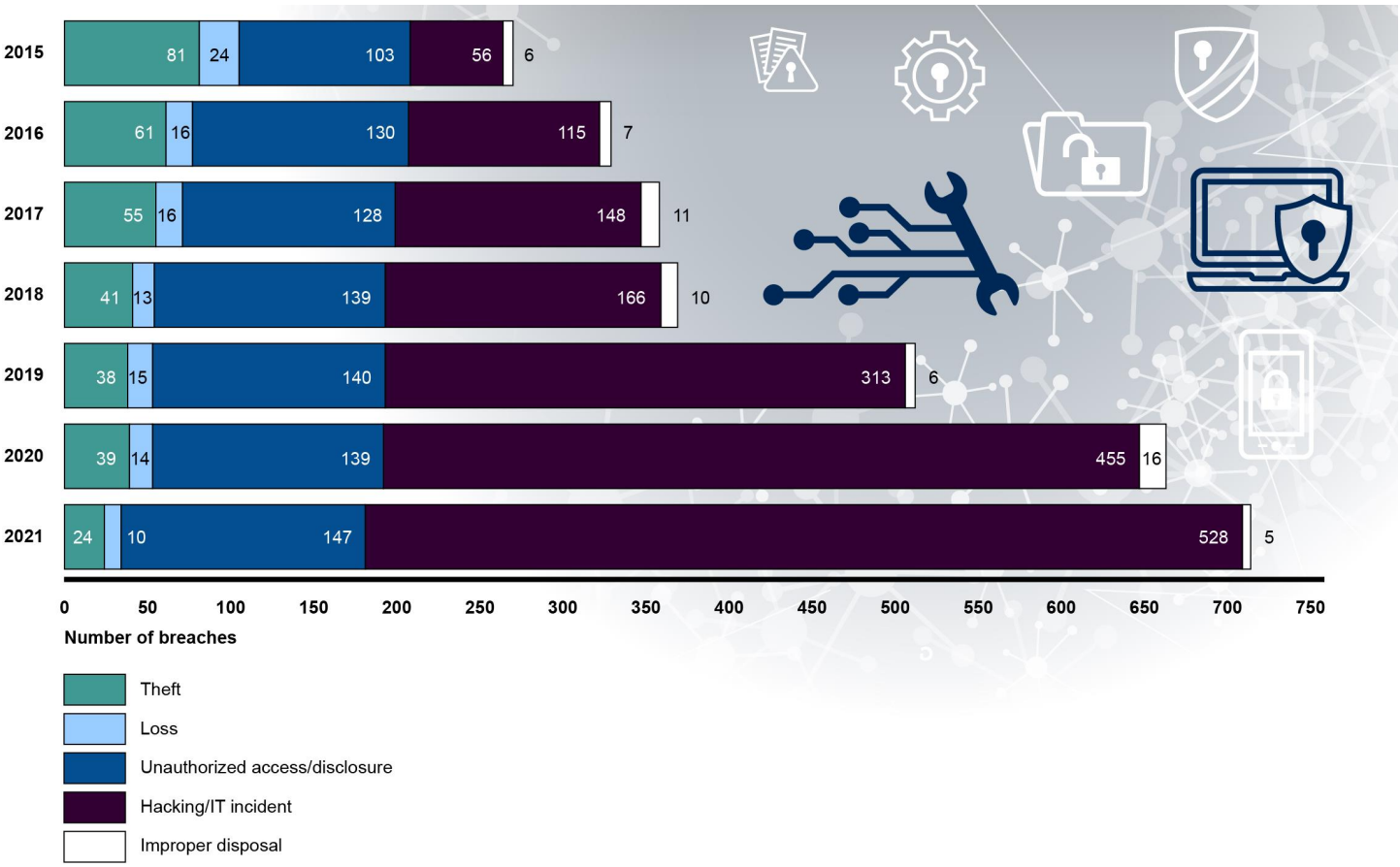
Figure 4: Number of Breaches Involving Unsecured Protected Health Information Reported by Covered Entities and Business Associates by Breach Type from 2015 to 2021



Source: GAO analysis of Department of Health and Human Services' January 2022 data; images: bearsky23/stock.adobe.com, Chor muang/stock.adobe.com. | GAO-22-105425

According to OCR's breach data, hacking and IT incidents have significantly increased by 843 percent since 2015. Similarly, unauthorized access and disclosure have increased by 43 percent since 2015. See Figure 5 for the trends in the various types of breaches that the covered entities and business associates reported since 2015.

Figure 5: Number of Breaches Involving Unsecured Protected Health Information by Breach Type from 2015 to 2021



Source: GAO analysis of Department of Health and Human Services' January 2022 data; images: bearsky23/stock.adobe.com, Chor muang/stock.adobe.com. | GAO-22-105425

Regarding the trends in the reported breaches from 2015 to 2021, OCR's Deputy Director for Health Information Privacy stated that covered entities and business associates reported email as a common attack vector among the breaches. The Deputy added that OCR had observed a lack of multifactor authentication as a common factor among entities that experienced a breach.[30] The Deputy also stated that since 2015, ransomware has been an increasingly common type of hacking and IT incident reported by covered entities and business associates.

[30]Multifactor authentication involves using two or more factors to achieve authentication. Factors include something you know (password or personal identification number), something you have (cryptographic identification device or token), or something you are (biometric). The combination of identification and authentication—such as user account-password combinations—provides the basis for establishing accountability and for controlling access to the system.

Specifically, the Deputy Director stated that in 2016, covered entities and business associates reported 36 ransomware attacks, while in 2020, 199 were reported. One example of a recent ransomware attack occurred in October 2020, in which employees from the University of Vermont Medical Center, a health care provider, could not access EHRs, payroll programs, and other vital digital tools for nearly a month. This attack reportedly cost University of Vermont Medical Center between $40 million and $50 million, mostly in lost revenue.[31]

The Number of Individuals Affected by Reported Breaches Have Varied since 2015

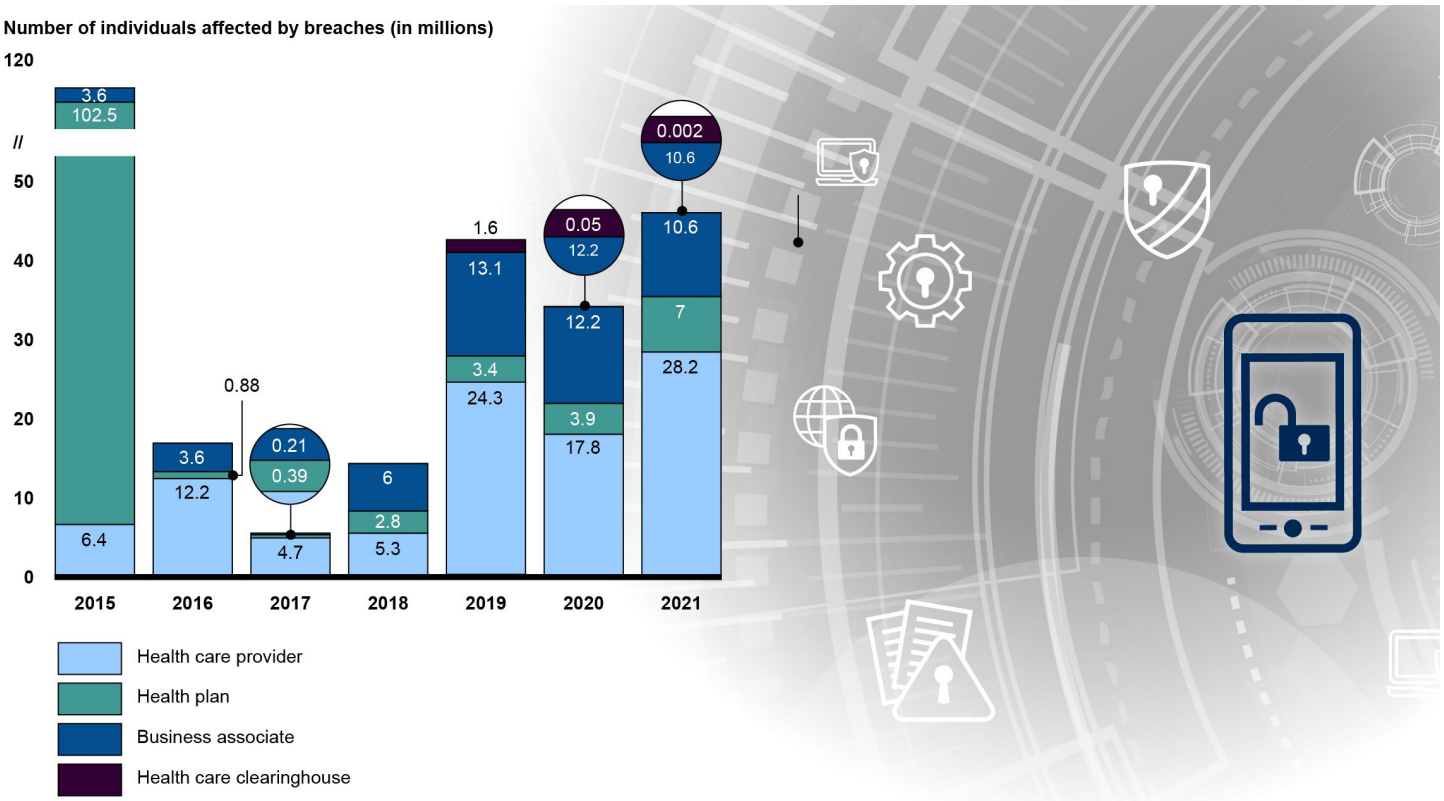
According to OCR's breach data, the number of individuals affected by breaches has varied each year since 2015. The data indicated approximately 270 million individuals have been affected by the approximately 3,200 breaches reported from 2015 to 2021.[32] Although breaches among health plans affected a significant number of people in 2015, since that time, breaches among health care providers have affected the most number of individuals.[33] For example, the number of individuals affected by breaches among the health care providers was approximately 58 percent of the total number of individuals affected from 2016 to 2021. Figure 6 shows the number of individuals affected by breaches for each type of covered entity and business associates each year from 2015 to 2021.

[31]Grace Bennighoff, "Malware on employee's company computer led to cyber attack on UVM Medical Center," VTDigger (July 21, 2021), (accessed February 25, 2022) https://vtdigger.org/2021/07/21/malware-on-employees-company-computer-led-to-cyber-attack-on-uvm-medical-center/.

[32]According to OCR, individuals may have been affected in multiple breaches either within the same year or multiple years. This makes it difficult to pinpoint a specific number of affected individuals.

[33]In 2015, two large breaches involving health plans—Anthem Inc. and Premera Blue Cross—affected a total of 102 million individuals, which is approximately over five times the number of individuals affected by breaches reported by health plans from 2016 to 2021.

Figure 6: Number of Individuals Affected by Breaches Involving Unsecured Protected Health Information from 2015 to 2021



Source: GAO analysis of Department of Health and Human Services' January 2022 data; images: bearsky23/stock.adobe.com, Chor muang/stock.adobe.com. | GAO-22-105425

The Deputy Director for Health Information Privacy stated that, among other reasons, the number of individuals affected by breaches may have increased because there has been a substantial increase in large breaches—those that affected 500 or more individuals. The Deputy Director stated that another reason for the increase in the number of individuals affected by breaches could be the rise in the number of business associates, who may hold data from many covered entities and become targets.

The following are examples of breaches involving unsecured PHI and PII affecting a significant number of individuals from 2015 to 2021:

- In January 2022, Broward Health, a health care provider, reported that a malicious intruder gained unauthorized access to the hospital's network and patient data through a third-party medical provider. The hackers reportedly accessed PII and PHI including banking

information, Social Security numbers, patient histories, and treatment and diagnosis records of approximately 1.3 million individuals.

- In July 2019, the American Medical Collection Agency, a business associate that specializes in small-balance medical-debt collection, reported a breach that involved the potential unauthorized access to an internal network. The attackers potentially accessed PII and PHI, including Social Security numbers, diagnoses, and credit card information, which affected approximately 21 million individuals.
- In January 2015, Anthem, Inc., a health plan, reported that a large-scale cyberattack on its IT systems had affected approximately 79 million individuals with Anthem accounts and those who received health care services in any of the areas that Anthem serves. The cyber attackers obtained PII and PHI such as names, dates of birth, Social Security numbers, health care ID numbers, and income data.
- In January 2015, Premera Blue Cross, a health plan, discovered that cyber attackers had gained unauthorized access to its IT systems. Approximately 11 million individuals were affected and the attackers accessed PII and PHI such as Social Security numbers, medical claims information, and bank account information.

HHS Is Taking Steps to Establish a Process to Review Recognized Security Practices during Investigations

As previously mentioned, the Enforcement Rule sets out requirements and procedures governing HHS's investigatory authority and the ability to impose civil money penalties on covered entities. In addition, the HITECH Act requires HHS to provide for periodic audits to ensure that covered entities and business associates comply with the HIPAA Rules.

Section 13412 of Public Law No. 116-321 (hereafter referred to as the "HITECH Amendment"), enacted in January 2021, amends the HITECH Act and adds a provision about recognized security practices. It states that when HHS is making determinations related to fines, audits, or remedies to resolve potential violations of the Security Rule, HHS shall consider whether the covered entity or business associate has

adequately demonstrated that it had implemented recognized security practices for the previous twelve months.[34]

In response to the Act's requirements, OCR's Deputy Director for Health Information Privacy stated that the office has taken several steps to finalize its process for considering whether covered entities and business associates have implemented recognized security practices at the conclusion of an investigation. For example:

- **Finalized standard operating procedures.** In March 2022, OCR's Director approved standard operating procedures for investigators to use when reviewing recognized security practices. Once the investigative process has concluded and if potential HIPAA security violation were found, recognized security practices are considered as a mitigating factor that may affect the resolution agreement, corrective action plan, or impositions of civil monetary penalties. The procedures are aimed to improve the consistency of how OCR's investigators request and consider whether covered entities and business associates have implemented recognized security practices by providing specific steps and guidance.
- **Published a request for information to seek public comments.** In April 2022, OCR published a request for information in the Federal Register, to seek public input, including from the health care sector, on how recognized security practices are being implemented. The request for information also seeks input on recognized security practices that are not specifically referenced in the HITECH Amendment that OCR should consider at the conclusion of an investigation, including those involving a breach. OCR's Deputy Director for Health Information Privacy stated that OCR intends to use the information collected to develop future guidance to assist regulated entities in improving the cybersecurity and safeguarding of the electronic PHI they hold.
- **Conducting outreach on the process.** OCR's Deputy Director for Health Information Privacy stated the request for information is intended to serve as a mechanism to officially communicate to the health care sector and raise awareness regarding the process to

[34]HITECH sec. 13412, Pub. L. No. 116-321 Stat. 5072. The HITECH Amendment defines standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology Act, the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015, and other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities.

consider recognized security practices at the conclusion of an investigation, including those involving a breach. In addition, OCR has added information on recognized security practices to its presentation materials, and the Deputy Director stated that the office is beginning to schedule public webinars, including a specific one on recognized security practices, by June 2022.

OCR plans to finalize the review process for considering whether covered entities and business associates have implemented recognized security practices no later than the summer of 2022. If the office can complete the associated tasks in the expected timeframe, covered entities and business associates would have more information available on the process and in turn may be better equipped to prepare for OCR's breach investigations.

OCR Lacks a Mechanism for Soliciting Feedback from Covered Entities on Its Processes

Federal law and policy emphasize the importance of coordination and collaboration among federal agencies, other levels of government, and the private sector to manage risks to the nation's critical infrastructure and other assets.[35] For example, the National Infrastructure Protection Plan (National Plan) includes sharing timely, actionable information about risks from significant threats and hazards to physical and cyber critical infrastructure, requiring an integrated approach to

- identify, deter, detect, disrupt, and prepare for threats and hazards to the nation's critical infrastructures, including the health care sector;
- reduce vulnerabilities of critical assets, systems, and networks; and

[35]See: Department of Homeland Security, National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience (Washington, D.C.: December 2013) and Presidential Policy Directive/PPD-21, Critical Infrastructure Security and Resilience (Feb. 12, 2013). The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Fiscal Year 2021 NDAA), Pub. L. No. 116-283, 134 Stat. 3388, 4770 (2021). Section 9002 of the NDAA added a new section 2215 to the Homeland Security Act of 2002, Sector Risk Management Agencies, which requires those agencies to coordinate with other federal departments and agencies, as well as with critical infrastructure owners and operators (codified at 6 U.S.C. § 665d).

- mitigate the potential consequences to critical infrastructure of incidents or adverse events that do occur.[36]

As previously mentioned, OCR is charged with implementing and enforcing the HIPAA Rules, including the development and management of the breach reporting process. As part of its responsibilities, OCR established a breach notification process.

OCR does not have a method for covered entities focused on providing feedback on the breach reporting process nor did the office indicate that it had plans to develop one. The Deputy Director for Health Information Privacy stated that the primary method for the office to receive information is through a breach investigation and that there is no formal process or platform for a covered entity or business associate to provide feedback. In addition, he noted that if a covered entity or business associate experienced issues during the breach reporting process, it could take one of three steps—schedule a meeting, email OCR at its publicly-available email address, or write a letter to OCR.

The National Plan emphasizes the importance of partners collectively adapting based on feedback and the changing environment. The plan states that recognizing the value of different perspectives helps the partnership more distinctly understand challenges and solutions related to critical infrastructure security and resilience. The plan also emphasizes that a well-functioning partnership, among other attributes, depends on clear and frequent communication.

As previously noted, we are not able to generalize the results of the survey we conducted of covered entities and business associates. Further, we had a low response rate for the survey that further diminishes the overall value of the results.

Nevertheless, the responses received provide useful insights. For example, most respondents indicated that the data breach reporting process was efficient. Of 89 responses received, 49 agreed or strongly agreed that the reporting process was efficient, while 17 disagreed or

[36]The National Plan defines critical infrastructure partners as Federal, State, local, tribal, and territorial governmental entities, public and private sector owners and operators and representative organizations, regional organizations and coalitions, academic and professional entities, and certain not-for-profit and private volunteer organizations that share responsibility for securing and strengthening the resilience of U.S. critical infrastructure.

strongly disagreed; the remaining 23 neither agreed nor disagreed, or did not know.

Respondents were less positive on communication-related challenges to the breach reporting process. Specifically, 70 of 88 respondents indicated there were communication-related challenges to the breach reporting process, while 4 said there were not; the remaining 14 did not know. Respondents provided a variety of suggestions on how OCR can improve communication and feedback on its breach reporting process. These suggestions ranged from providing a platform to submit anonymous questions to establishing a method to directly solicit feedback from the health care sector members.

Without a clear mechanism to provide feedback to OCR, covered entities and business associates may face challenges during the breach reporting process. Further, soliciting feedback on the breach reporting process could help OCR improve or simplify aspects of the process and may decrease long lapses of communication during ongoing breach reporting investigations.

Conclusions

While the increasing use of health IT systems have the potential to improve health care quality, they can be vulnerable to the loss or unauthorized disclosure of PII and PHI. Breaches experienced by covered entities and their business associates have resulted in hundreds of millions of individuals having sensitive information compromised.

OCR is taking steps to finalize its process to considering whether covered entities and business associates have implemented recognized security practices. These efforts, if implemented within the expected timeframes, may help improve the consistency of the breach investigations process and better prepare covered entities and business associates for investigations.

OCR has not provided a formal method for covered entities and business associates to provide feedback to about the breach reporting and investigations processes. Addressing this shortcoming will be an important step toward improving or simplifying aspects of the breach and investigations process and preventing long lapses of communication during ongoing breach reporting investigations.

Recommendation for Executive Action

The Secretary of HHS should ensure that OCR establishes a mechanism for covered entities and business associates to provide feedback on OCR's breach reporting process. (Recommendation 1)

Agency Comments

We provided a draft of this report to HHS for review and comment. In its response reproduced in appendix II, HHS generally concurred with our recommendation and stated that it would take actions to implement it. Specifically, HHS officials stated that OCR will solicit feedback related to the breach reporting process when covered entities and business associates submit a breach notification.

In its response, HHS noted that OCR will establish a mechanism for regulated entities to provide feedback on the breach reporting and investigative process. Specifically, OCR plans to add language and contact information to the confirmation email that regulated entities receive when they submit breach reports through the HHS Breach Portal to invite feedback and questions about the breach reporting process. The agency also plans to implement procedures for OCR's regional offices to regularly review and address emails received about the breach reporting process through their respective mailboxes. We will continue to follow-up with HHS to validate its implementation of this recommendation.

HHS also provided technical comments, which we have incorporated in the report, as appropriate.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to the appropriate congressional committees, the Secretary of the Department of Health and Human Services, and other interested parties. In addition, the report will be available at no charge on the GAO website at http://www.gao.gov.
If you or your staff have questions about this report, please contact Jennifer R. Franks at (404) 679-1831 and Marisol Cruz Cain at (202) 512-5017. They can also be reached by e-mail at franksj@gao.gov and cruzcainm@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report.

GAO staff who made major contributions to this report are listed in appendix III.

Jennifer R. Franks
Director, Center for Enhanced Cybersecurity
Information Technology & Cybersecurity Team

Marisol Cruz Cain
Director
Information Technology & Cybersecurity Team

Appendix I: Objectives, Scope, and Methodology

The objectives of our review were to examine

1. the number of breaches and affected individuals covered entities have reported to HHS since 2015;
2. the extent to which HHS established a review process to assess whether covered entities had implemented recognized security practices; and
3. the extent to which improvements can be made related to HHS's breach reporting requirements.

To address our first objective, we reviewed and analyzed prior GAO reports that identified security and privacy threats to data and information systems. Further, we analyzed information provided by HHS on the number of unsecured protected health information breaches affecting 500 or more individuals.[1] To determine the reliability and accuracy of the data, we obtained and analyzed answers to nine data reliability questions that addressed the internal controls of the system used to collect the data. Specifically, we asked questions about the system that had collected and maintained the data, to determine whether it had procedures in place to consistently and accurately capture data, access controls over the data, and system changes. In addition, to verify that the data did not include obvious errors such as missing data fields or unexplained outliers, our analysis was confirmed by a second analyst and our team's methodologist. Through these steps, we determined that the data were sufficiently reliable for our purposes.

For our second objective, we reviewed relevant information security and privacy laws, including the Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health (HITECH) Act, and Public Law No. 116-321 (that amended the

[1]Under the Health Insurance Portability and Accountability Act of 1996 and the Breach Notification Rule, a covered entity must notify HHS of a breach that affected more than 500 individuals within 60 calendar days of discovery. OCR investigates each these breaches. For breaches that affect less than 500 individuals, the reporting requirement changes to 60 days after the end of each calendar year and investigations are initiated at HHS's discretion.

HITECH Act) to identify HHS's responsibilities related to considering recognized security practices. Further, we interviewed knowledgeable OCR officials to discuss the steps taken to consider recognized security practices during investigations and reviewed documentation, where available, to verify the actions.

For our third objective, we compared OCR's breach reporting process against leading practices to determine the extent to which OCR's efforts aligned. Subsequently, we interviewed OCR officials to gain a better understanding of their process and any efforts underway to address the flaws in their process. In addition, we interviewed the Chief Security Officer of the Health Information Sharing and Analysis Center and the Executive Director for Cybersecurity of the Healthcare and Public Health Sector Coordinating Council to discuss their views on OCR's breach reporting process.

Lastly, we developed a survey to gather the perspectives of covered entities and business associates to better understand their perspectives on OCR's breach reporting process. The GAO survey questions were distributed by the Health Information Sharing and Analysis Center (approximately 5,000 individuals from 700 firms globally), Healthcare and Public Health Sector Coordinating Council (approximately 660 individuals from 332 organizations), and the American Hospital Association (approximately 43,000 individuals from approximately 5,000 health care organizations). The respondents to our survey were self-selected and while the results cannot be generalized to the entire population of covered entities and business associates, the results do allow us to learn in detail about the actual experiences of many different types of covered entities and business associates.

We conducted this performance audit from September 2021 to May 2022 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the Department of Health and Human Services

DEPARTMENT OF HEALTH & HUMAN SERVICES — OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

May 10, 2022

Jennifer R. Franks
Director
Information Technology & Cybersecurity Team
Center of Enhanced Cybersecurity
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Ms. Franks:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, "***Electronic Health Information: HHS Needs to Improve Communications for Breach Reporting***" (Job code 105425/GAO-22-105425).

The Department appreciates the opportunity to review this report prior to publication.

Sincerely,

Melanie Anne Egorin

Melanie Anne Egorin, PhD
Assistant Secretary for Legislation

Attachment

GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED — Electronic Health Information: HHS Needs to Improve Communications for Breach Reporting(GAO-22-105425)

The U.S. Department of Health & Human Services (HHS) appreciates the opportunity from the Government Accountability Office (GAO) to review and comment on this draft report.

General Comments

Recommendation 1

The Secretary of HHS should ensure that OCR establishes a mechanism for covered entities and business associates to provide feedback on OCR's breach reporting process.

HHS Response

HHS Concurs with GAO's recommendation.

To address GAO's recommendation, OCR will establish an additional mechanism for regulated entities to provide feedback to OCR on the breach reporting and investigative process. Specifically, OCR will:

1. Add language to the confirmation email that regulated entities receive when they submit breach reports through the HHS Breach Portal to expressly invite their feedback and questions about the breach reporting process. Each confirmation email will include an email address for the OCR regional office that is conducting the investigation.
2. Implement procedures for OCR's regional offices to regularly review and address emails received about the breach reporting process through their respective mailboxes.

Agency Comment Letter

Text of Appendix II: Comments from the Department of Health and Human Services

May 10, 2022

Jennifer R. Franks
Director
Information Technology & Cybersecurity Team
Center of Enhanced Cybersecurity
U.S. Government Accountability Office
441 G Street NW

Washington, DC 20548

Dear Ms. Franks:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, "Electronic Health Information: HHS Needs to Improve Communications for Breach Reporting" (Job code 105425/GAO-22-105425).

The Department appreciates the opportunity to review this report prior to publication.

Sincerely,

Melanie Anne Egorin, PhD
Assistant Secretary for Legislation

Attachment

GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED — Electronic Health Information: HHS Needs to Improve Communications for Breach Reporting (GAO-22-105425)

The U.S. Department of Health & Human Services (HHS) appreciates the opportunity from the Government Accountability Office (GAO) to review and comment on this draft report.

General Comments

Recommendation 1

The Secretary of HHS should ensure that OCR establishes a mechanism for covered entities and business associates to provide feedback on OCR's breach reporting process.

HHS Response

HHS Concurs with GAO's recommendation.

To address GAO’s recommendation, OCR will establish an additional mechanism for regulated entities to provide feedback to OCR on the breach reporting and investigative process. Specifically, OCR will:

1. Add language to the confirmation email that regulated entities receive when they submit breach reports through the HHS Breach Portal to expressly invite their feedback and questions about the breach reporting process. Each confirmation email will include an email address for the OCR regional office that is conducting the investigation.

2. Implement procedures for OCR’s regional offices to regularly review and address emails received about the breach reporting process through their respective mailboxes.

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

Jennifer R. Franks, (404) 679-1831, franksj@gao.gov
Marisol Cruz Cain, (202) 512-5017, cruzcainm@gao.gov

Staff Acknowledgments

In addition to the individuals named above, Keith Kim (analyst-in-charge), Gerard Aflague, Chris Businsky, Donna Epler, Andrew Knox, David Matcham, Monica Perez-Nelson, Scott Pettis, and Walter Vance made significant contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548