COSMOS
Navigate the Compliance Universe

Health Care Privacy Compliance Handbook, 3rd Edition
5. Payer Privacy Issues

By Debbie R. Mabari [1]

Introduction

What is privacy? Or perhaps more importantly, does privacy still exist in today's interconnected world? Many people view the Fourth Amendment to the Constitution of the United States as implicitly granting a right to privacy:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath...[2]

Most people, therefore, believe that their right to privacy is a given, underscored by law.

However, as computerized data storage and analysis by both private and public organizations become ever more widespread, we have seen a significant erosion in individual privacy.

Thankfully, privacy protections are alive and well when it comes to personal healthcare data. This chapter will explore the impact of privacy regulations in the data-driven payer sector—organizations that provide health insurance and other managed care services.

As discussed in earlier chapters, the U.S. government recognizes the need to safeguard health information separate and apart from other personal information, particularly through the Health Insurance Portability and Accountability Act (HIPAA), which created a set of national standards and practices to safeguard *protected health information* (PHI). Those who must comply with these rules and standards are *covered entities.* Organizations in the payer sector fall primarily in the covered-entity category of *health plan.*[3]

Under HIPAA and related rules, covered entities must protect an individual's PHI collected or created as a result of healthcare operations. See Chapter 1, "HIPAA Privacy and Security," for a deep dive into the wide range of HIPAA requirements. This chapter focuses on key privacy principles that arise with health plans.

Key Principles

Privacy vs. Security

While privacy compliance is much broader than what is in the HIPAA regulations, it is particularly important for payer organizations to be able to distinguish between HIPAA privacy and HIPAA security issues and ensure each are independently addressed.

HIPAA privacy focuses on the right of consumers to control the use of their information. It is also responsive to the expectation of consumers that sensitive information a health plan or provider has about their personal life is only available to the appropriate persons. PHI cannot be used or divulged by others against the consumer's wishes, except where allowed by regulation. The Privacy Rule covers PHI in all formats, including electronic,

paper, and oral, and aims to protect confidentiality—an assurance that information will be safeguarded from unauthorized disclosure.

HIPAA security refers to the methods used to protect the confidentiality of all sensitive information that is transmitted and stored at a health plan or in the custody of those who contract with the health plan, including providers and downstream entities. The Security Rule details how covered entities are expected to ensure the confidentiality, integrity, and availability of electronic PHI (ePHI). The Security Rule also focuses on administrative, technical, and physical safeguards and protection of ePHI from unauthorized access, whether external or internal, stored or in transit.

Portability and Interoperability: *All in One Place*

Before we further explore the privacy mandates that payers have, we should consider a contrasting concept—health data portability. Portability is a term that describes the process or accessing relevant member or patient data remotely, and then utilizing that data locally to support and inform care, as well as improve the member and patient experience. Portability of PHI is a critical component to improving consumer experience by linking the data between insurance companies, hospitals, and physicians, as well as pharmacies and ancillary providers. It allows patients and providers to have access to up-to-date and informed healthcare information across the entire spectrum.

The focus on true portability received a boost in the spring of 2018 from Centers for Medicare & Medicaid Services (CMS) Administrator Seema Verma:

> Imagine a world if you're collecting all of your health-care data from the time of birth all the way through your life.... We want to get to a point where patients have all of their health-care information in one place.[4]

Interoperability is the term used to describe how portability of data is managed across disparate systems. Interoperability typically involves one or more application programming interfaces (APIs) or *bridges* between systems that take data from one source and map that data to an unrelated recipient software application. The use of APIs and other sophisticated data exchange tools is critical to creating an experience that behaves as if consumers have *all their healthcare information in one place.*

There are significant privacy concerns and challenges that come to the forefront as soon as general portability and interoperability are mandated. For example, health information is now being collected and shared across a wide range of mobile and consumer devices, many of which do not meet the standards required for HIPAA-related sharing of PHI. When HIPAA was enacted in 1996, the proliferation of smartphones and tablets along with their ubiquitous apps, plus an exponential increase in the amount of stored and shared data, was unanticipated. The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009,[5] which provided updates to HIPAA, set additional standards for the collection, storage, and sharing of medical records and health-related information across covered entities, but does not discuss personal or consumer devices.

So, we are at an important crossroads, where the need to protect patient privacy will be continually weighed against the need to make health information accessible across the entire healthcare spectrum. Constantly changing technology and greater information-sharing capabilities may force legislation to keep pace with these privacy challenges.

Collection, Use, and Disclosure

The HIPAA Privacy Rule allows for some uses and disclosure of PHI and ePHI without an authorization from the consumer, namely for treatment, payment ,and healthcare operations (TPO).[6] Each of these areas will be discussed in detail below, but it is important to note that if a use or disclosure is not permitted, then the information can only be used or disclosed with documented permission and in accordance with the direction of the consumer. Consumers can also request that their personal information be shared with a third party who is their designated representative (e.g., a spouse or parent). Another key provision related to collection, use, and disclosure is the *minimum necessary standard*, which establishes that covered entities must not collect, use, or disclose more personal information than what is needed to accomplish a particular task.[7] This concept is also discussed in detail below.

Treatment, Payment, Healthcare Operations

Treatment includes the provision, coordination, or management of healthcare and related services among healthcare providers or by a healthcare provider with a third party, consultation between healthcare providers regarding a patient, or the referral of a patient from one healthcare provider to another. While such disclosures may be minimal for a health plan, some examples of where it may be applicable include coordination of care efforts, consultation between providers, and referrals to another provider.[8]

Payment includes activity undertaken by the health plan to obtain premiums, to fulfill responsibility for the provision of benefits under the health plan, and to obtain or provide reimbursement for the provision of healthcare. Some examples of payment activities applicable to a plan include determining eligibility or coverage under a plan; adjudicating claims, risk adjustments, billing and collection activities; and utilization review activities.[9]

And finally, the Privacy Rule defines *healthcare operations* as activities compatible with and directly related to conducting quality assessments and improvement activities for the health plan as well as case management, resolving grievances, coordination of care activities, and credentialing. Underwriting, insurance rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits are also considered healthcare operations. Conducting or arranging for a medical review, legal services, and auditing functions, such as fraud and abuse detection, are also activities that allow for use and disclosure by the health plan.[10]

Marketing and Health Plans

Understanding the definition of *marketing* under the HIPAA Privacy Rule is important across the industry, but even more so with health plans, as the marketing department of a health plan helps drive its sales which in turn drive revenue. There are important controls that address whether and how PHI may be used and disclosed for marketing.[11] In general, a written authorization is needed to use PHI for marketing. However, there are some exceptions that health plans should be aware of and which may be important to a health plan's mission of ensuring consumers or beneficiaries receive important information that relates to quality-of-care issues.

It is important to first define what constitutes marketing under the rule. The Privacy Rule defines marketing as making a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.[12] Simply put, a covered entity may not sell PHI to a business associate or any third party for that party's own purposes. Health plans also may not sell lists of consumers or beneficiaries to third parties without first obtaining an authorization from each person on the list. This part of the definition has no exceptions. An example of marketing that fits the above description would be a health plan that sells a list of its members to a third party that sells blood glucose monitors. The third party purchased the information with

the intent to send the plan's members brochures on the benefits of purchasing and using the monitors. This information cannot be sold without an authorization from every member on the list.

Once marketing is defined, the next step is to identify and understand what marketing is not. The Privacy Rule establishes exceptions to the marketing rules in the following areas:[13]

1. **Refill Reminders**: It is not considered marketing if the communication is made to provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the consumer; however, if any financial remuneration is received from a third party for making the communication, it must be reasonably related to the health plan's cost of making the communication. For example, a covered entity cannot profit from making the particular communication.

2. **Health-Related Products or Services**: It is not considered marketing if a health plan communication describes a health-related product or service (or payment for such product or service) that is already provided by, or included in the consumer's existing plan of benefits of, the covered entity making the communication. This includes communications about:

    a. The entities participating in a healthcare provider network or health plan network;

    b. The replacement of, or enhancements to, a health plan; and

    c. Health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits. For example, a health plan may inform members about its own products and services in situations such as communications describing a disease management program that is available to the consumer at no cost.

3. **Treatment, Case Management, or Care Coordination Purposes**: It is not considered marketing if a healthcare provider contacts a consumer as part of the consumer's treatment plan. This area is less applicable to health plans and has more impact on pharmacies or healthcare providers. For example, a provider may contact his/her patient to suggest alternative treatment options, therapies, or other providers.

These additional factors should be considered when reviewing exceptions to the marketing requirements:

- The activity must otherwise be permissible under the Privacy Rule.
- A health plan cannot receive financial remuneration directly or indirectly from a third party whose products or services are being described.
- When using vendors or delegates, a health plan should ensure that a business associate agreement is in place and that the vendor uses the PHI only for communication activities intended by the health plan.

An excellent resource for understanding the practical application of the Privacy Rule, whether about marketing, the minimum necessary standard, or any other provision, is the Frequently Asked Questions section of the U.S. Department of Health & Human Services (HHS) website.[14]

Privacy and HIPAA/HITECH Compliance for Health Plans

Privacy and security practices under HIPAA/HITECH and related compliance for a health plan can be broken down into two categories, each with different considerations:

- Internal systems and processes that use and maintain control of data within an organization.

- External services and functions that involve *First-Tier, Downstream, and Related* entities (FDRs) and that require additional audit and chain of custody controls.

Management of PHI within a covered entity fundamentally involves:

- Protecting the privacy of patient information.
- Securing patient health information (physically and electronically).
- Adhering to the minimum necessary standard for use and disclosure of patient health information.
- Specifying patients' rights for access, use, and disclosure of their health information.

Minimum Necessary Standard

"For uses of protected health information, the Covered Entity's policies and procedures must identify the persons or classes of persons within the Covered Entity who require access to the information to carry out their job duties, the categories or types of protected health information needed, and conditions appropriate to such access."[15]

One significant challenge within most organizations is that data are highly compartmentalized or *siloed* within different departments or functional areas. Therefore, maintaining control over PHI is made more difficult by having to monitor multiple systems and processes that include similar or duplicate consumer data. When data are replicated and stored in many places, it becomes more difficult to ensure that data are being updated, purged, and maintained across all parts of the organization.

Whether using or viewing PHI or ePHI from an internal or external source, one of the more important concepts in the HIPAA Privacy Rule is the minimum necessary standard (see sidebar). The standard is intentionally lacking in specific detail, because CMS wants each covered entity and business associate to develop criteria and implement policies and procedures appropriate for its own organization, reflecting the entity's business practices and workforce, and does not want to hinder timely access to quality healthcare.

It is important to note that the minimum necessary standard does not apply to the following:

- Disclosures to or requests by a healthcare provider for treatment purposes.
- Disclosures to the consumer who is the subject of the information.
- Uses or disclosures made pursuant to a consumer's authorization.
- Uses or disclosures required for compliance with the HIPAA Administrative Simplification rules.
- Disclosures to HHS when disclosure of information is required under the Privacy Rule for enforcement purposes.
- Uses or disclosures that are required by other law.

Contracting and Management of FDRs

In the *Medicare Managed Care Manual* (*MCMG*),[16] for health plans that provide Medicare Advantage (MA) plans,

the contracting and management of FDRs are explicitly detailed. Essentially, all FDRs, with few exceptions, are considered an extension of the covered entity and are accountable to the plan for meeting and maintaining the same HIPAA/HITECH privacy regulations, standards, and guidance as internal users. Note that the *MCMG* states:

> The MA organization agrees to take **ultimate responsibility** [emphasis added] for all services provided and terms of the contract and otherwise fulfilling all terms and conditions of its contract with CMS regardless of any relationships that the organization may have with entities, contractors, subcontractors, first-tier or downstream entities.[17]

For a health plan, this means that contracts with FDRs must include an executed *business associate agreement* stating that the organization will have access to PHI, how it will be used, and that all PHI must be used according to the minimum necessary standard (described above), including the return or destruction of PHI once the need for it is completed. Keep in mind that the business associate/FDR has the same obligations under HIPAA/HITECH as the covered entity. Most importantly, however, the health plan organization is **ultimately responsible** for overall compliance.

Definitions[18]

First-Tier Entity: Any party that enters into a written arrangement with a health plan to provide administrative services or healthcare services for a Medicare-eligible individual.

Downstream Entity: Any party that enters into a contract with the first-tier entity. These written arrangements continue down to the level of the ultimate provider of health and/or administrative services.

Related Entity: Any entity that is related to the MA organization by common ownership or control and performs some of the MA organization's management functions or furnishes services to Medicare enrollees under an oral or written agreement or leases real property or sells materials to the MA organization.

Every FDR/business associate with access to PHI is tasked with ensuring that all HIPAA administrative, technical, and physical safeguards are in place. FDRs and business associates must comply with the HIPAA Privacy Rule, including required audit and reporting functions to the covered entity. In addition, should there be an *incident* or *breach*, there must be compliance and/or contract documentation in place that details the notification, control, investigation, and corrective action required. The associated HIPAA Security Rule details the requirements for safe handling of ePHI *at rest* (storage), along with how ePHI must be managed *in transit* (transfer or communications).

A pre-delegation compliance audit, including a comprehensive risk analysis, is required to determine and assess whether an FDR meets the HIPAA/HITECH administrative, technical, and physical requirements. The risk analysis is a broad-scope, organization-wide analysis of systems, facilities, and processes aimed at identifying threats or weaknesses that might expose PHI or ePHI. Once these vulnerabilities are exposed, the organization can develop and implement corrective actions that will reduce or eliminate the potential for PHI breaches and related incidents.[19]

Data at Rest, In Transit, and In Use

Regardless of whether data are used internally or across different entities, great care must be taken to encrypt protected data with HIPAA-approved algorithms to assure that, if data are ever accessed (intentionally or accidentally), they are not stored in clear text and are instead unreadable and untranslatable.[20] With regulatory and company obligations to store data history anywhere from seven to ten years, encrypting data storage is essential. Data in transit via website, secure FTP, or API exchanges must also be encrypted to prevent the communication lines from being compromised or data from being recorded as they are transferred between systems and across the internet.

The less data are needed, used, or accessed, the more security can be leveraged to protect them. The more data are needed, used, or accessed, the less secure they may be in order for people and systems to efficiently use and process them. For example, you cannot print encrypted data on a member's letter since the member will not be able to read them.

Additional physical and digital protections must be put in place at the print location to secure the printed text once it is printed on a readable piece of paper. In this digital age, it is easy to forget that physical paper trails also represent high-risk areas that can lead to incidents and breaches of protected data. In some cases, paper is even more difficult to protect, since anyone can read it without first entering a username or password.

This point serves as a good segue to review another common *low-tech* mode of communication: oral discussion. Talking on the phone in public about a member's health conditions represents data in transit that are not properly encrypted and not easily protected, except by educating and managing human behavior.

Further stewardship is outlined by HIPAA to properly deidentify and dispose of protected data. Deidentification processes and procedures involve removing or reconfiguring the 18 HIPAA identifiers (see Chapter 1 for the full list) with a specific algorithm so that data can be further protected during storage and transmission and reidentified later by following the same algorithm in reverse when those data are needed again.

When physical or digital data and the associated hardware and devices used to store them become obsolete or too old to maintain, HIPAA and other compliance standards identify the appropriate means of destruction. Physical media like paper and laptops must be securely shredded or destroyed and unable to be reconstituted. Typically, digital data requires a more intense process of purging any residual remnants of data from both the hard drive and memory sectors of devices.

All the regulations and considerations for the appropriate handling of protected data make it critical to have robust policies and procedures around data identification, use, and disclosures. These documents should lay out each data type, how and when it is allowed to be used, how it is to be protected at all times during the process of servicing a consumer, and how and when it is allowed to be communicated given the minimum necessary standard.

Privacy Breaches: Far-Reaching and Costly Consequences

A robust privacy compliance program with clearly documented policies and procedures is essential to health plan operations in a much more general way than just regulatory oversight. Privacy breaches have an adverse impact on health plans in a variety of ways—loss of customer goodwill, tarnished reputation in the marketplace, increased regulatory scrutiny, private lawsuits, potential fines and penalties, and the time and expense of mitigating future occurrences and notifying customers, consumers, and regulators. To understand the concept of what constitutes a breach and what happens if one occurs, see Chapter 2, "Breach Notification."

Having a robust privacy compliance program sends the message to consumers that there is a strong commitment to protecting personal information. Additionally, the ability to demonstrate an effective privacy compliance program can potentially mitigate the amount of penalties and/or fines a health plan might have to pay in the event of a privacy breach. In many cases, a health plan may be more concerned about the negative impact a privacy breach will have on its business and reputation than the fine or penalty itself.

Privacy violations may carry civil and criminal penalties under HIPAA/HITECH, as well as applicable state laws. See Chapter 1 for specifics on enforcement penalties.

Recently, HHS has demonstrated its ongoing vigilance to enforcement of the Privacy Rules, with 2018 standing out as a record year: *In 2018, OCR settled 10 cases and secured one judgment, together totaling $28.7 million. This total surpassed the previous record of $23.5 million from 2016 by 22%.*[21]

Some recent examples of privacy breaches and their resulting settlements and media coverage provide a clear and cautionary picture of the extent to which fines, penalties, and settlements can add up not only in financial terms, but also from a public relations perspective as well:

- In 2017, one of the largest U.S. health plans sent two mailings to 12,000 plan members using oversized windowed envelopes through which it was possible to see members' names, addresses, and their HIV-positive status. The insurance company settled a class-action lawsuit for more than $17 million and paid more than $2 million in settlements and fines to five states and the District of Columbia for the impermissible disclosure of PHI.
- In 2017, a New England-based Medicare Advantage and Medicaid plan settled with OCR for more than $1.2 million after the company impermissibly disclosed PHI of up to 344,579 people by returning multiple photocopiers to a leasing agent without erasing data on the copier hard drives.
- In 2018, a large, multi-state health plan paid $16 million to OCR to settle HIPAA violations resulting after cyberattacks led to the largest US health data breach in history and exposed the ePHI of almost 79 million people.

While these and other rulings clearly indicate the commitment of HHS to safeguard consumer privacy, in 2019, the agency's continuous process of evaluation and interpretation of the HIPAA/HITECH rules was evident in an interim final rule regarding enforcement discretion of civil monetary penalties that reduced the maximum annual penalty in three of the four enforcement tiers, as outlined in Table 1.

Table 1: Penalty Tiers Under the Enforcement Rule and Under Notification of Enforcement Discretion[22]

Culpability	Minimum Penalty/Violation	Maximum Penalty/Violation	Annual Limit	
			Under Enforcement Rule	Under Enforcement Discretion (2019)
No Knowledge	$100	$50,000	$1,500,000	$25,000

Reasonable Cause	1,000	50,000	1,500,000	100,000
Willful Neglect – Corrected	10,000	50,000	1,500,000	250,000
Willful Neglect – Not Corrected	50,000	50,000	1,500,000	1,500,000

Security and Privacy vs. Ease of Doing Business—Cost vs. Convenience

Most security and privacy programs must meet a minimum set of standards in order to be both effective and compliant. This greatly increases the cost of doing business. But as illustrated by the settlements described above, financing the prevention of data breaches may be preferable and more affordable than dealing with the financial penalties and damage to reputation that can come with the data breach itself. But will there come a point in the future where compensating for such situations becomes counterproductive? Some may look at their information technology and security budgets and suggest that we have already reached that point. If not, that day may soon arrive.

The goal to move to a *centralized global data record* where an individual's PHI can be accessed all in one place could serve to intensify the *Fort Knox* approach since **all** critical private data would be stored in one place with a single point of entry for both authorized users and nefarious players.

Security programs help to keep the bad guys out, but they can keep everyone else out, too. It's important to realize that an overly intense security program can have the reverse effect on trust and confidence if it stands in the way of convenience. If it becomes too difficult for a healthcare consumer to gain access to health information, to get affordable healthcare, or to make payments or process claims accurately, the end result could be frustration, withdrawal, or—in the worst-case scenario—loss of access to timely and appropriate care.

At the same time, the ongoing proliferation of mobile and online technologies has led many consumers to inadvertently open locked doors to their private information by blindly accepting end-user agreements. Often, these end-user agreements are from multiple independent sources and thus represent multiple unintended points of entry. Much like a dam that has sprung several leaks, putting your finger in one hole does not eliminate any of the other leaks or improve the structural integrity of the dam itself.

Dauntingly, *easy* and *secure* are two words that are rarely used in the same sentence. But as technology becomes more advanced and the growing needs of healthcare become increasingly complex, these two concepts will have to reach some level of equilibrium—so consumers have access to timely and appropriate care, and secured entities can maintain cost-effective businesses.

Proactive Experience vs. Invasion of Privacy

Our current level of technology can seem truly amazing with advances that have taken place just in the last several years, and yet, at times, it can seem a little creepy, too. The ability of the algorithms behind your home assistant to listen, analyze, and make intelligent suggestions can result in a positive consumer experience,

followed up by an unwanted personal ad on your social media page. At what point does the portability and interconnectivity of personal data and personal human interactions become too invasive? To some, we may already have crossed that line.

But as the healthcare industry moves toward more centralization of PHI, advanced technology has an opportunity to provide a more positive impact. For example, similar algorithms to those used for identifying the *next most likely purchase* could be applied to centralized PHI and medical history to identify when a patient is due for a preventive screening, when a health plan member will likely hit the plan deductible, or what interventions would be most advantageous for an individual managing a chronic condition.

Individualized healthcare—tailoring interventions to a specific patient's needs, right down to the level of his or her DNA—has been gaining momentum as a potentially positive future state for medical treatment. In a similar way, personal data preferences may be able to offer guidance to regulators, industry leaders, and consumers regarding access to and the use and disclosure of the PHI included in a centralized global data record.

Summary

In summary, the focus on sensitive information by advocacy groups and legislative leaders continues to increase, resulting in the adoption of more federal and state laws and regulations. The public and political pressures are driven by headlines about privacy breaches, which means regulatory scrutiny and enforcement will likely continue to increase. A robust privacy and security program is essential in helping a health plan identify the key compliance principles.

Health plans must also be committed to educating and informing employees, business associates, and consumers about the key compliance risks identified as well as what is being done to address those risks. A compliance oversight committee consisting of the organization's leadership team must play a role in assessing the risk and setting risk tolerance for the health plan.

This chapter began with a discussion about privacy in general, went on to outline the key principles of HIPAA privacy that affect health plans, and finally offered reflection on the current and possible future states of privacy considerations in light of continual advances in technology. No matter what lies ahead, a key to mitigating privacy risks in any scenario is to integrate an effective and efficient privacy compliance program with the health plan's business priorities, thereby holding business leaders accountable and responsible for safeguarding consumers' information.

1Debbie R. Mabari is Chief Executive Officer for Cody Consulting Group, Inc. in Tampa, FL.
2 U.S. Const. amend. IV.
345 C.F.R. § 162.103 .
4 Bertha Coombs, "Medicare chief says it's time health care caught up to other industries to benefit consumers," *CNBC*, April 30, 2018, https://www.cnbc.com/2018/04/30/cms-verma-says-its-time-health-care-caught-up-to-other-industries.html.
5 Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, § 13,001, 123 Stat. 226 (2009).
645 C.F.R. § 164.506 .
745 C.F.R. §§ 164.502(b), 164.514(d) .
845 C.F.R. § 164.501 .
945 C.F.R. § 164.501 .
1045 C.F.R. § 164.501 .
1145 C.F.R. §§ 164.501, 164.508(a)(3) .

1245 C.F.R. § 164.501 .
1345 C.F.R. §§ 164.501, 164.508(a)(3) .
14 "HIPAA FAQs for Professionals," Health Information Privacy, U.S. Department of Health & Human Services, last reviewed October 12, 2017, https://www.hhs.gov/hipaa/for-professionals/faq/index.html.
15 "Minimum Necessary Requirement," Health Information Privacy, U.S. Department of Health & Human Services, last reviewed July 26, 2013, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement/index.html.
16 CMS, *Medicare Managed Care Manual*, Pub. No. 100-16.
17 CMS, *Medicare Managed Care Manual,* ch. 11 § 110.1.
18 CMS, *Medicare Managed Care Manual,* ch. 21 § 20.
19 CMS, *Medicare Managed Care Manual,* ch. 21 § 50.
20 "Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals," Health Information Privacy, U.S. Department of Health & Human Services, last reviewed July 26, 2013, https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html.
21 "OCR Concludes 2018 with All-Time Record Year for HIPAA Enforcement," Health Information Privacy, U.S. Department of Health & Human Services, last reviewed February 7, 2019, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/2018enforcement/index.html.
22 Notification of Enforcement Discretion Regarding HIPAA Civil Money Penalties, 84 Fed. Reg. 18,151 (April 30, 2019) , https://www.federalregister.gov/documents/2019/04/30/2019-08530/notification-of-enforcement-discretion-regarding-hipaa-civil-money-penalties.