Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

HIPAA, Telehealth, and COVID-19

June 5, 2020

In recent years, health care providers have increasingly turned to technology to provide remote health care services to patients (*i.e.*, "telehealth"). This use of telehealth has only become more important in the midst of the coronavirus disease 2019 (COVID-19) pandemic, as it has allowed providers and patients to minimize their contact with one another. However, the use of technology to transmit information carries privacy risks. Federal law thus limits the extent to which health care providers may use technology to transmit medical information. In particular, the Health Insurance Portability and Accountability Act (HIPAA) requires covered entities—namely, health care providers, health plans, and health clearinghouses—to abide by data privacy, data security, and data breach notification requirements in their treatment of certain medical information. While HIPAA's restrictions mitigate privacy and security concerns, they also limit health care providers' ability to offer telehealth services. Given the increased need for telehealth options due to COVID-19, the Department of Health and Human Services (HHS) has announced that it will not enforce HIPAA's requirements against health care providers who are engaged in the good-faith provision of telehealth services during the COVID-19 emergency, regardless of whether those service are related to COVID-19.

This Sidebar provides a high-level overview of this issue. It first discusses the scope of HIPAA's requirements and how those requirements apply to telehealth. It then describes the actions HHS has taken to provide relief from these requirements during the COVID-19 pandemic.

HIPAA's Requirements

General Overview

HIPAA imposes obligations on health care providers and other "covered entities," including health plans and health clearinghouses, regarding their transmission of "protected health information" (PHI). PHI includes information that (1) "identifies," or can reasonably "be used to identify," an individual; (2) is "created or received by a health care provider, health plan, employer, or health care clearinghouse"; (3) relates to an individual's physical or mental health, health care provision, or payment for provision of health care; and (4) is transmitted by or maintained in electronic or any other format.

Under HIPAA, health care providers must treat PHI consistent with requirements set forth in several HHS regulations known as the "Privacy Rule," the "Security Rule," and the "Breach Notification Rule." The

Congressional Research Service
https://crsreports.congress.gov
LSB10490

Privacy Rule limits covered entities' use and sharing of PHI with third parties without valid patient authorization, unless a specific HIPAA exception applies. One such exception applies when a covered entity shares PHI with a "business associate"—a category of entities discussed below. The Security Rule requires covered entities to maintain administrative, physical, and technical safeguards to prevent threats or hazards to the security of electronic PHI. The technical safeguards must include transmission security measures designed to "guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network." These measures must have "integrity controls" to ensure the electronically transmitted PHI is "not improperly modified without detection until disposed of" and mechanisms "to encrypt electronic protected health information whenever deemed appropriate." Under the Breach Notification Rule, covered entities must, upon discovery of a breach of "unsecured" PHI (*i.e.*, any PHI not rendered unreadable or unusable), notify affected individuals within 60 calendar days. They must also notify the Secretary of HHS, and, for certain large breaches, the media. The Breach Notification Rule defines a "breach" broadly as the "acquisition, access, use, or disclosure of protected health information in a manner not permitted under [HIPAA's privacy regulations] which compromises the security or privacy of the protected health information."

Violations of HIPAA can lead to civil or criminal enforcement action. The HHS Office of Civil Rights (OCR) is responsible for investigating and enforcing civil violations of HIPAA's requirements. Penalties range from $100 per violation (with a maximum of $25,000 per year for "identical" violations, meaning violations of the "same requirement or prohibition in one of the HIPAA rules or in the statute") up to $50,000 per violation (with a maximum of $1,500,000 per year for identical violations), depending on the violator's culpability. OCR also refers possible criminal violations of HIPAA to the Department of Justice (DOJ), which has criminal enforcement authority under the statute. DOJ may seek fines or imprisonment against a person who "knowingly" obtains or discloses "individually identifiable health information" or "uses or causes to be used a unique health identifier" in violation of HIPAA's requirements.

Business Associates

HIPAA's requirements apply not only to covered entities, but also to their "business associates." The business associate category is particularly relevant in the context of telehealth because, as discussed in the next section, many third-party vendors involved in the provision of telehealth services, such as videoconference providers, may qualify as business associates. A business associate is defined as any person who, on behalf of a covered entity, "creates, receives, maintains, or transmits protected health information" for a HIPAA-covered transaction. HHS has recognized an exception for services that act as mere "conduits" for the delivery of PHI, such as the U.S. Postal Service and internet service providers. However, according to HHS, this exception is "narrow" and applies only to capture entities providing "mere courier services" and who do not access the information "other than on a random or infrequent basis as necessary to perform the transportation service or as required by other law." The exception does not apply to any entity that "maintains" PHI on behalf of a covered entity, beyond temporary storage incident to transmission, "even if the entity does not actually view the PHI."

Covered entities may share PHI with business associates only if they first enter into a written contract with the business associate that provides "satisfactory assurances" the business associate will "appropriately safeguard the information." This contract must "[e]stablish the permitted and required uses and disclosures of protected health information by the business associate," and it may not authorize the business associate to use or further disclose the PHI in a manner that, if done by a covered entity, would violate HIPAA's requirements.

Not only will covered entities violate HIPAA if they fail to enter into a HIPAA-required contract with a business associate, but business associates themselves are directly liable under HIPAA. Regardless of the terms of the contract—and, according to HHS, even if there is no contract—an entity that meets HIPAA's

business associate definition must comply with HIPAA's Privacy, Security, and Breach Notification Rules and is directly liable for violating them.

Application to Telehealth

As detailed in CRS Report R46239, *Telehealth and Telemedicine: Frequently Asked Questions*, by Victoria L. Elliott, telehealth involves the use of information and communication technology to deliver clinical and nonclinical health care services. Telehealth service often is provided through "four common telehealth modalities": (1) "clinical video health or live video"; (2) "mobile health," which allows providers to deliver materials through a patient's mobile application; (3) "remote patient monitoring," in which a provider furnishes "daily case management services for the patient's chronic medical conditions"; and (4) "store-and-forward technology," by which a provider uses a health information technology system to exchange information related to a patient's medical record.

Because the use of these modalities typically requires the electronic transmission of PHI by third parties that provide the technologies, health care providers must comply with HIPAA's privacy, security, and breach notification requirements when providing telehealth services. Thus, under the Privacy Rule, a health care provider may not provide a patient's PHI to a third-party vendor, such as a video conferencing provider, unless it obtains authorization from the patient or an exception applies. If a provider wishes to rely on the business associate exception, it must first enter into a business associate contract with the vendor. Under the Security Rule, providers must have controls in place to prevent any unauthorized access to or modification of PHI during its electronic transmission. Relatedly, if a provider is using a business associate to transmit the PHI electronically, the business associate contract must provide "satisfactory assurances" that the business associate will "appropriately safeguard the information." Lastly, under the Breach Notification Rule, health care providers must notify any affected patients within 60 calendar days after discovering a "breach" of "unsecured" PHI.

These requirements apply not only to health care providers, but also to entities that operate telehealth technologies who meet HIPAA's business associate definition. Under HIPAA, a third party that provides the technology used in telehealth, such as videoconferencing technology, is a business associate if it stores PHI or sends or receives it without acting merely as a "conduit." For instance, a video communications service that stores communications on its own computer server—beyond "temporary storage incident to transmission"—would likely qualify as a business associate because they are "maintain[ing]" the PHI. These vendors must comply with HIPAA's privacy, security, and data breach notification requirements, even if they have not entered into a formal contract with a health care provider.

Application of HIPAA Requirements to Health Care Providers During the COVID-19 Emergency

Although health care providers must typically comply with HIPAA's requirements, HHS has said it will use its enforcement discretion to provide temporary relief in response to the COVID-19 pandemic. As detailed in this Report, federal agencies enjoy discretion in deciding whether to bring enforcement actions, and courts generally decline to review such decisions. Given this discretion, the HHS OCR has announced that during the COVID-19 public health emergency it is "exercising its enforcement discretion" not to enforce the HIPAA rules against health care providers providing telehealth services in good faith.

In its notice of enforcement discretion, OCR explained that health care providers may use "non-public facing audio or video communications products" such as "Apple FaceTime, Facebook Messenger video chat, Google Hangouts video, Zoom, or Skype" without the risk that OCR will seek a penalty for HIPAA

non-compliance. OCR encourages providers to notify patients of the potential privacy risks of these platforms, and also to enable all privacy modes and encryption where available. OCR noted, however, that health care providers who seek "additional privacy protections" should provide such services through technology vendors that are HIPAA compliant and will enter into business associate contracts. It identified several vendors—such as Skype for Business, Zoom for Healthcare, and Google G Suite Hangouts Meet—who have represented that they are HIPAA compliant and willing to enter into business associate contracts, although OCR disclaimed that it was validating any of the vendors' HIPAA compliance. OCR said, however, that health care providers should not use public-facing services such as "Facebook Live, Twitch, TikTok," and similar "public-facing" applications, and it further explained in a separate publication that use of these services could be evidence of "bad faith" subject to enforcement. OCR's notice of enforcement discretion does not have an expiration date, and OCR has said that it will notify the public when it no longer applies.

DOJ, unlike OCR, has not declared that it will refrain from exercising its criminal enforcement authority during the COVID-19 emergency. Consequently, individuals may still be liable for "knowingly" obtaining or disclosing PHI in violation of HIPAA's requirements. However, while OCR did not address criminal liability in its notice of enforcement discretion, it might choose not to refer cases to DOJ for criminal prosecution that involve a health care provider relying in good faith on OCR's notice of enforcement discretion.

Author Information

Chris D. Linebaugh
Legislative Attorney

Disclaimer