Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated December 4, 2024

Cybersecurity and Digital Health Information

As the technologies used in health care expand, so too do cybersecurity vulnerabilities. Increasingly, health care actors use electronic health records (EHRs), artificial intelligence (AI) technologies, and telehealth services to provide and facilitate care. While these technologies have their advantages, stakeholders have noted they also increase the number of potential cybersecurity vulnerabilities an entity may be exposed to through greater technological complexity and the number of actors with which an entity may interact.

Cyberattacks targeting sensitive health information maintained by health care providers and health plans have sharply increased over the past decade. Health care data and information are valuable and therefore are an attractive target for cyberattacks. Cybersecurity experts predict that cyberattacks involving health information will continue to affect a growing number of people in the future.

Health care providers, health plans, and health care clearinghouses that hold or transmit electronic protected health information (e-PHI) are subject to the Health Insurance Portability and Accountability Act (HIPAA; P.L. 104-191) Security Rule and Breach Notification Rule. These HIPAA rules are administered and enforced by the Office for Civil Rights (OCR) within the Department of Health and Human Services (HHS). OCR works with other HHS agencies to provide guidance and compliance tools for HIPAA-covered entities.

Any breach of unsecured protected health information (PHI) must be reported to OCR pursuant to the Breach Notification Rule. A breach is the "acquisition, access, use, or disclosure of protected health information in a manner not permitted under the [HIPAA Rules] which compromises [its] security or privacy." Protected health information is *unsecured* if it "is not rendered unusable, unreadable, or indecipherable to unauthorized persons" (such as through encryption).

There are generally five types of digital breaches reported to OCR: a hacking or information technology (IT) incident of electronic equipment or a network server, unauthorized access to or disclosure of records containing PHI, theft of electronic equipment/portable devices, loss of electronic media, and improper disposal of PHI. During 2022, OCR was notified of 626 breaches where each affected 500 or more people, the majority of which were hacking incidents. Over 41 million people were affected by these breaches. OCR was notified of 63,966 breaches affecting fewer than 500 people during the same period, with the most common cause being unauthorized access to, or disclosure of, PHI. 257,105 people were affected by these breaches.

HIPAA

HIPAA was enacted to "improve the efficiency and effectiveness of the health care system," in part by ensuring that patients have access to their health information and establishing privacy and security measures for such data. Pursuant to HIPAA, several rules were promulgated, including the Privacy Rule, the Security Rule, and the Breach Notification Rule—the latter two are especially important for e-PHI. The HIPAA Rules apply to covered entities that possess PHI or e-PHI, such as health care providers, health plans, health care clearinghouses, and business associates.

HIPAA Security Rule. Issued in 2003, the HIPAA Security Rule "establishes national standards to protect individuals' [e-PHI] that is created, received, used, or maintained by a covered entity." The Security Rule enumerates 18 administrative, physical, and technical safeguards (or standards) for e-PHI to ensure its confidentiality, integrity, and security. These standards are designed to be flexible and scalable to entities of all sizes, as well as technology neutral, so that entities may adopt novel technologies as they emerge.

Covered entities and business associates have discretion in how they accomplish the 18 standards, depending upon the organization's "size, complexity and capabilities," its "technical infrastructure, hardware, and software security capabilities," the "costs of security measures," and the "probability and criticality of potential risks to [e-PHI]." Each security standard is accompanied by one or more implementation specifications. Specifications may be required, meaning an organization *must* implement them, or addressable, meaning an organization *may* implement equivalent alternative measures if reasonable and appropriate. For example, the security management process standard is accompanied by four required implementation specifications, one of which is a risk analysis. Every covered entity and business associate must "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of [e-PHI]" in its possession. This analysis is the foundation of all other safeguards in the Security Rule. OCR has published guidance and jointly released a HIPAA Security Risk Assessment (SRA) Tool with the Assistant Secretary for Technology Policy/Office of the National Coordinator for Health Information Technology (ASTP/ONC) to help entities properly conduct this risk analysis. The National Institute of Standards and Technology (NIST) and OCR also collaborated on a revised special publication that in part provides guidance on how to conduct this risk analysis.

The HIPAA Security Rule has faced criticism. A primary current stakeholder concern is that it does not apply broadly enough in the context of emerging technologies. Some entities, such as personal health application developers, may receive e-PHI yet fall outside the rule's scope. Stakeholders question whether such entities will use or disclose sensitive data for marketing and other purposes. Similar concerns have been raised regarding data used to train, validate, and test AI models. Other critiques include that the Security Rule insufficiently addresses cybersecurity threats such as ransomware. The Spring 2024 Unified Agenda indicates OCR anticipates publishing a proposed rule to strengthen the HIPAA Security Rule shortly.

HIPAA Breach Notification Rule. Introduced in 2009, the HIPAA Breach Notification Rule requires covered entities and their business associates to notify select parties following an unsecured PHI breach. A breach is generally assumed when there has been an impermissible use or disclosure of PHI, unless an exception is met or the entity performs a risk assessment that demonstrates a low probability that PHI has been compromised. Typically, business associates must notify their corresponding covered entities upon discovery of a breach. In turn, generally, if a breach affects 500 people or more, a covered entity must timely notify individuals affected and the HHS Secretary, who must publish a list of such breaches on the HHS website. Additionally, if more than 500 individuals in a particular state or jurisdiction are affected by a breach, prominent media outlets serving those regions must be notified by the covered entity. Conversely, if fewer than 500 people are affected, generally a covered entity must timely notify individuals affected and the Secretary.

Similar breach notification provisions under the Federal Trade Commission (FTC) Health Breach Notification Rule (HBNR) apply to vendors of personal health records (PHRs) and related entities not already subject to HIPAA. The FTC has stated that the HBNR encompasses health applications and other connected device companies.

Medical Device Cybersecurity

Device software functions regulated by the U.S. Food and Drug Administration (FDA), which have proliferated in recent years, include software as a medical device (SaMD) and software that is a component of a device. Many such devices are "cyber" devices; that is, they may connect to the internet and networks to facilitate patient care, increasing the devices' susceptibility to cyberattack. Large hospitals may have thousands of networked devices running on multiple software platforms, increasing opportunity for unauthorized access to health data. Responsibility for the cybersecurity of medical devices has been an ongoing concern for stakeholders, with medical device manufacturers and device users sometimes unclear about the locus of responsibility for ensuring device cybersecurity. Traditionally, FDA addressed device cybersecurity through its existing authorities (i.e., Quality System [QS] Regulation, 21 C.F.R. Part 820) and guidance on both premarket and postmarket device cybersecurity. In 2022, Congress established requirements for premarket submissions for *cyber devices*, including for 510(k) notifications, de novo requests, and premarket approval applications (PMAs), among others (Consolidated Appropriations Act, 2023; P.L. 117-328). Device sponsors are required to "design, develop, and maintain processes and procedures to provide a reasonable assurance that the device and related systems are cybersecure" and to include in their premarket submissions "a plan to monitor, identify, and address, as appropriate, in a reasonable time, postmarket cybersecurity vulnerabilities" and a software bill of materials, among other things (Federal Food, Drug, and Cosmetic Act § 524B). FDA, in a draft March 2024 guidance document, outlined proposed updates to its existing final premarket cybersecurity guidance to address requirements under FFDCA Section 524B for cyber devices.

Considerations for Congress

Myriad government actions targeting the cybersecurity of digital health information have been proposed, undertaken, issued, and enacted. Select examples include the Cybersecurity Act of 2015 (P.L. 114-113, Division N) and the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA; P.L. 117-103, Division Y). Section 405 of the Cybersecurity Act of 2015 (Improving Cybersecurity in the Health Care Industry) tasked HHS with multiple actions to assess and strengthen cybersecurity in the health care industry, including the creation of a health care industry cybersecurity task force. Section 405(d) required HHS to create common, voluntary guidelines and best practices, methodologies, procedures, and processes to combat cybersecurity risks in the health care and public health (HPH) sector.

As the scale of cyberattacks in the United States against the HPH sector has increased, both domestic and foreign parties have been implicated. According to stakeholders, the outcomes of these cyberattacks (often due to ransomware) can include hospital closures, regional health care delivery disruptions, and potentially even patient deaths. The seriousness of disruptions to care delivery was illustrated by the Change Healthcare cyberattack and subsequent bills introduced in the 118th Congress (see, e.g., S. 5218 and S. 5390). Approaches that may be considered to strengthen cybersecurity in the HPH sector might include, among others, modification of existing regulatory requirements; coordination and communication between cybersecurity and health agencies; resource allocation, for example, grants to health care facilities; and regularly updated communications (e.g., guidance documents), for example, to focus on rural facility readiness, as these facilities may have limited resources to invest in cybersecurity measures.

Additionally, there is no comprehensive digital data protection law in the United States. While OCR may enforce the HIPAA rules and FTC may enforce the HBNR, stakeholders have noted confusion regarding their applications, especially as technologies evolve. In addition, states may have varying data privacy and security laws. Furthermore, although many data protection guidance documents are available, they are voluntary.

Nora Wells, Analyst in Health Policy
Amanda K. Sarata, Specialist in Health Policy

Disclaimer