



February 12, 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 weaknesses 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. Cybersecurity experts predict that cyberattacks involving health information will continue to affect a growing number of people in the future. This In Focus reviews the implications of cybersecurity on health information.

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 or disclosure of records containing PHI, theft of electronic equipment/portable devices, loss of electronic media, and improper disposal of PHI. During 2021, OCR was notified of 609 breaches where each affected 500 or more people, the majority of which were hacking incidents. Over 37 million people were affected by these breaches. OCR was notified of 63,571 breaches affecting fewer than 500 people during the same period, with the most common cause being unauthorized access to, or disclosure of, PHI. Over 300,000 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 ePHI 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 Office of the National Coordinator for Health Information Technology (ONC) to help entities properly conduct this risk analysis. The National Institute of Standards and Technology (NIST) and OCR have also been collaborating on a revised special publication that would, in part, discuss 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.

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. 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. In turn, 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. Responsibility for the cybersecurity of medical devices has been an ongoing concern for stakeholders, with medical device manufacturers and device users often 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 2023, 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).

Considerations for Congress

Myriad government actions targeting, in whole or in part, 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, entitled Improving Cybersecurity in the Health Care Industry, of the Cybersecurity Act of 2015 in particular tasked HHS with multiple actions to assess and strengthen cybersecurity in the health care industry. Within Subsection (d) of Section 405 specifically, HHS was also granted the authority 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.

Further considerations for Congress exist regarding the cybersecurity of digital health information. Select considerations include issues related to the scale of cyberattacks and their outcomes, limited and patchwork privacy and security governance, and a lack of cybersecurity resources available to different parties.

Regarding the scale of cyberattacks in the United States against the HPH sector, both domestic and foreign parties have been implicated. Some cyberattacks against this sector have also been attributed to nation-states. According to stakeholders, the outcomes of these cyberattacks (often due to ransomware) include hospital closures, regional health care delivery disruptions, and potentially even patient deaths. Consequently, some stakeholders have suggested that such cyberattacks should be considered and treated as regional disasters.

No comprehensive digital data protection law exists in the United States. While OCR may enforce HIPAA 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 guidances are available, they are voluntary.

Additionally, there is inequity in access to cybersecurity resources among health care actors. Rural and smaller health care facilities in particular may not have the funds to maintain a cybersecurity workforce or regularly update their technologies and cybersecurity measures. In general, the cybersecurity workforce is already limited, making it particularly difficult for rural and smaller providers to attract and retain qualified staff.

Nora Wells, Analyst in Health Policy

Amanda K. Sarata, Specialist in Health Policy

IF12591

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.