SIDLEY

SIDLEY UPDATE

Digital Health Industry Take Note: New HIPAA Comment Opportunity and Guidance Addresses Growing Risk of Cybersecurity Attacks

May 3, 2022

Digital health companies should take note of new data privacy and security developments under the Health Insurance Portability and Accountability Act (HIPAA) that can affect product planning and customer negotiations.

The U.S. Department of Health and Human Services Office for Civil Rights (OCR) has released a request for information (RFI) seeking input on (1) how covered entities implement recognized security practices, which OCR considers in enforcement matters and (2) the different types of harm that individuals experience from HIPAA violations in order to consider how OCR may share enforcement recoveries with individuals harmed. Digital health companies subject to HIPAA should consider submitting comments by the June deadline to ensure that the evolving digital health industry has a voice in establishing industry best practices and advocating for continued flexibility in the implementation of security standards that suit their unique business needs distinct from traditional covered entities and business associates.

Digital health companies should also consider undertaking an impact analysis of OCR's recent industry newsletter for HIPAA–regulated entities to protect against some of the more common cyberattack techniques.

What is Digital Health?

There is no singular definition of "digital health," which is used as an umbrella term to describe a wide range of businesses, many regulated by HIPAA and some of them not. For example, some digital health companies are treatment providers, billing health insurers electronically for services offered through artificial intelligence technology, and thus regulated under HIPAA as covered entities. Other digital health companies may be business associates, such as those that provide data analytics or support platforms that assist in core healthcare provider or life sciences functions such as clinical trial recruitment or population-based medication management software for integrated delivery networks or health insurers. Yet still other digital health companies, such as certain wellness or behavioral health apps, may be

unregulated under HIPAA but may face questions from large employer customers as to whether the technology offering is “HIPAA compliant.” The examples go on and on.

The key is to recognize that businesses that fall under the rubric of digital health often have specific obligations under HIPAA and, even if not, carry a burden to demonstrate HIPAA-like compliance as a cost of doing business in the healthcare industry.

RFI Regarding Recognized Security Practices

Earlier this month, OCR released an RFI seeking public input on two requirements of the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act), as amended. Specifically, the HITECH Act requires the Department of Health and Human Services (HHS) to take into account recognized security practices when determining potential fines, audit results, or other remedies for resolving potential HIPAA violations and requires HHS to establish a methodology under which an individual harmed by a HIPAA violation may receive a percentage of any civil money penalty. Accordingly, the RFI seeks comments on (1) how covered entities and business associates are implementing recognized security practices and how they anticipate demonstrating such practices are in place and (2) the types of harm individuals experience as a result of HIPAA violations. The RFI supports HHS’s overall focus on developing enhanced safeguards of electronic personal health information (ePHI) in the fight against cybersecurity threats.

Comments from digital health companies could help inform what should be considered a recognized practice and what should be considered industry practice in ePHI within the evolving and varied practices of digital health business platforms. Commenters should also consider addressing the types of relative harms individuals can experience from HIPAA violations that could result from the use of digital health and ensure that OCR understands key risk mitigation steps that digital health businesses can take that can reduce the potential effects of such harms on individuals. Comments must be submitted by June 6, 2022.

Cybersecurity Industry Newsletter

Last month, OCR issued an **industry newsletter** for HIPAA-regulated entities (i.e., covered entities and business associates) to take steps to protect against some of the more common cyberattack techniques. OCR highlighted three types of common cyberattacks — phishing emails, exploitation of known vulnerabilities, and weak authentication protocols — and noted the particular risks faced by the healthcare industry for such attacks.

Digital health companies should note this new HIPAA guidance that provides recommendations for ways to avoid common cybersecurity attacks. Even for digital health companies not subject to HIPAA, the guidance may become a best practice standard that customers may expect digital health companies to adopt.

As stated in OCR’s newsletter, the number of breaches of unsecured ePHI reported to the OCR affecting 500 or more individuals due to hacking or IT incidents increased 45% from 2019 to 2020. Further, the number of breaches due to hacking or IT **incidents** accounted for 66% of all breaches affecting 500 or more individuals reported to OCR in 2020. OCR concludes that most cyberattacks could be prevented or substantially mitigated if HIPAA-covered entities and business associates implemented HIPAA Security Rule requirements to address the most common types of attacks.

The standards and implementation specifications found in the HIPAA Security Rule provide a baseline for protecting ePHI. A regulated entity that fails to meet this baseline becomes an attractive soft target for hackers who can access ePHI by exploiting known vulnerabilities. For instance, weak password rules and single-factor authentication are among the practices that can contribute to frequent, successful attacks (over **80% of breaches** due to hacking involved compromised or brute-forced credentials). Accordingly, OCR's reminders and recommendations in the new guidance for HIPAA regulated entities include to

1. assess and reduce risks and vulnerabilities to the availability of ePHI, which is defined as "the property that data or information is accessible and useable upon demand by an authorized person" pursuant to the HIPAA Security Rule; see 45 CFR 164.308(a)(1)(ii)(A)-(B); see also 45 CFR 164.304 (definition of "Availability")
2. implement stronger authentication solutions, such as multifactor authentication
3. implement a security awareness and training program for all workforce members pursuant to the HIPAA Security Rule. 45 CFR 164.308(a)(5)(i); management personnel should also participate, as senior executives may have greater access to ePHI and are often **targeted** in phishing email attacks
4. **implement** a vulnerability management program that includes using a vulnerability scanner to detect vulnerabilities such as obsolete software and missing patches, and periodically conducting penetration tests to identify weaknesses that could be exploited by an attacker
5. implement a privileged access management system that is reasonable and appropriate to reduce the risk of unauthorized access to privileged accounts pursuant to the HIPAA Privacy Rule; see 45 CFR 164.312(a)(1)
6. pay careful attention to cybersecurity alerts describing newly discovered vulnerabilities
7. periodically examine the strength and effectiveness of their cybersecurity practices and increase or add security controls to reduce risk as appropriate pursuant to the HIPAA Privacy Rule; see 45 CFR 164.306(e)
8. **upgrade or replace** obsolete, unsupported applications and devices (legacy systems); however, if an obsolete, unsupported system cannot be upgraded or replaced, additional safeguards should be implemented or existing safeguards enhanced to mitigate known vulnerabilities until upgrade or replacement can occur

The newsletter demonstrates that HHS believes that covered entities and business associates "underappreciate the risks and vulnerabilities of their actions or inaction (e.g., increased risk of remote access, unpatched or unsupported systems, not fully engaging workforce in cyber defense)," demonstrating that the government may be aggressive where it views regulated entities as not taking necessary steps to protect ePHI.

Digital health companies should consider reassessing their processes to protect ePHI in light of the OCR newsletter. The latest HIPAA guidance from OCR adds to a growing body of government resources setting expectations for the obligations of regulated entities to mitigate the potential for cyberattacks on ePHI and may have broader reach in setting commercial expectations of customers entering into arrangements with companies that have access to health-related personal information.

CONTACTS

Elizabeth Hardcastle, Partner	+1 202 736 8697, ehardcastle@sidley.com
Meenakshi Datta, Partner	+1 312 853 7169, mdatta@sidley.com
Colleen Theresa Brown, Partner	+1 202 736 8465, ctbrown@sidley.com
Sama E. Kahook, Associate	+1 202 736 8674, skahook@sidley.com

---