DORSEY
DORSEY+WHITNEY LLP

Significant New Healthcare Privacy and Cybersecurity Developments

April 29, 2024 – Dorsey Health Law
by Ross C. D'Emanuele and Laura C.S. Newberry

As the federal government continues to take action in response to events impacting the healthcare landscape, stakeholders must ensure that they are staying up-to-date with health information privacy and security developments in the healthcare industry. This blog post summarizes two recent significant actions: a new HIPAA final rule and proposed federal cybersecurity legislation.

New HIPAA Final Rule

The U.S. Department of Health and Human Services ("HHS") has expressed concern about patient trust in the privacy of health care information since the U.S. Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization* in 2022. Most recently, on April 22, 2024, HHS's Office for Civil Rights ("OCR") issued a new final regulation under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy Rule: HIPAA Privacy Rule to Support Reproductive Health Care Privacy.

The final rule strengthens privacy protections for sensitive information about reproductive health care by:

- Prohibiting covered entities and their business associates from using or disclosing protected health information ("PHI") for the purpose of an investigation into or proceeding against an individual or entity who seeks, obtains, provides, or facilitates lawful reproductive health care, which includes providing information on or paying for any such services. This prohibition does not apply in situations of suspected abuse, neglect, or endangerment.

Related People

- Ross C. D'Emanuele
- Laura C.S. Newberry

Related Capabilities

- Healthcare & Life Sciences
- Healthcare Transactions & Regulations
- Healthcare Litigation
- Medical Devices

- Prohibiting covered entities and their business associates from identifying any individual or entity for the purpose of any such investigation or proceeding.
- Requiring covered entities and their business associates to obtain a signed attestation when they receive a request for PHI potentially related to reproductive health care for the purpose of health oversight activities, judicial or administrative proceedings, law enforcement, or coroner or medical examiner disclosures. The attestation must include the individual or class of individuals whose PHI is requested, the covered entity or business associate, the requestor, a statement that the PHI will not be used or disclosed for any prohibited purpose, and a statement acknowledging the criminal penalties for any violation of the Privacy Rule.
- Prohibiting a provider from refusing to treat a person as the personal representative of a patient merely because they provided or facilitated reproductive health care for a patient.
- Requiring covered entities to revise their Notice of Privacy Practices.

The final rule is scheduled for publication in the Federal Register on April 26, 2024. It will become effective 60 days after publication, with compliance to occur by February 16, 2026 for the Notice of Privacy Practices requirement and within 240 days after publication for all other requirements. As the compliance dates quickly approach, covered entities and business associates must ensure alignment of their policies, practices, and Notices of Privacy Practices with this new final rule. Covered entities and business associates may also need to revise their business associate agreements, to the extent that such agreements would permit a business associate's use or disclosure of PHI that is prohibited under the new rule.

Proposed Federal Cybersecurity Legislation

The healthcare industry has seen a recent increase in cybersecurity incidents. According to OCR, over the past few years, the number of large breaches reported and the number of individuals affected by those breaches have doubled. Now, following the Change Healthcare breach, Congress is considering new legislation: Health Care Cybersecurity Improvement Act of 2024 (S.B. 4054).

On March 22, 2024, Senator Mark R. Warner (D-VA), introduced the proposed federal legislation, which has been referred to the Senate Committee on Finance. Sen. Warner, who is a member of the Committee on Finance and co-founder and co-chair of the Senate Cybersecurity Caucus, is a well-known advocate of enhanced cybersecurity in the healthcare industry.

The proposed legislation charges the Secretary of HHS with setting minimum cybersecurity standards for Medicare's Accelerated Payment Program and Advance

Payments Program. During the COVID-19 public health emergency, the Centers for Medicare and Medicaid Services offered accelerated and advance payments to assist in disruptions to claims payments due to the public health emergency. Under the Health Care Cybersecurity Improvement Act of 2024, if a participating Part A hospital or one of its intermediaries does not meet the set standards, the hospital will not receive accelerated payments under the Accelerated Payment Program where a cybersecurity incident caused the disrupted operations or cash flow problems. Similarly, if a participating Part B provider or one of its intermediaries does not meet the set standards, the provider will not receive advance payments under the Advance Payments Program where a cybersecurity incident caused the delayed claims payments by health insurance companies. Notably, the accelerated and advance payments are only for Medicare Part A and Part B claims payments.

Currently, the bill is still in the early stages of the legislative process, and, if the law were enacted, enforcement would not occur until two years after its enactment. However, given the continuing prevalence of cybersecurity incidents in the healthcare industry, additional detailed HIPAA Security Rule cybersecurity guidance, as well as emerging state agency activity (such as New York's proposed cybersecurity regulations for hospitals), now is the time for healthcare providers and other covered entities and business associates to focus on HIPAA Security Rule compliance to protect against hacking, ransomware and other cybersecurity attacks, and the resulting disruptions to clinical care.

If you have any questions about the HIPAA Privacy Rule or Security Rule, proposed cybersecurity legislation, or their potential impact on you or your organization, please contact the authors or your regular Dorsey attorney.