Briefings on HIPAA

Balancing state laws and HIPAA requirements

by Dom Nicastro

Those in charge of overseeing HIPAA compliance at their healthcare organizations need to have a firm understanding of privacy laws outside of the healthcare arena.

Andrea Frey, co-chair of Hooper Lundy & Bookman's Digital Health Practice in San Francisco, watches this interplay closely. Her practice specializes in transactional and healthcare regulatory matters, with an emphasis on health privacy, digital health, licensure and certification, scope of practice, and medical staff issues. In this article, Frey discusses some of the key issues surrounding privacy laws and HIPAA.

Consumer privacy laws in the mix

Issue: The interplay between HIPAA and the state consumer data privacy laws such as the CCPA/CPRA, the Colorado Privacy Act, the Virginia Consumer Data Protection Act, and other relevant state laws that similarly extend privacy and security protections to health data.

Questions for HIPAA compliance officers: What should a HIPAA compliance officer do to fully grasp these data privacy laws and how they interplay with HIPAA? What steps should a HIPAA compliance officer take to understand which regulations take precedence and to address matters where HIPAA and data privacy laws cross?

Frey's advice: First, organizations should figure out if state-level consumer data privacy laws apply to them and the personal data they collect from consumers subject to the laws—though this isn't always a straightforward assessment.

Many of these laws contain exemptions for nonprofit entities and covered entities (CE) regulated by HIPAA or other health privacy laws (such as the Confidentiality of Medical Information Act [CMIA] in California). For example, any data that is already governed and protected by HIPAA would be excluded from the definition of personal information. (Note that the general applicability requirements of these laws and the scope of the laws' respective exemptions differ between states. National organizations will need to conduct a state-by-state analysis.)

Organizations must ensure compliance with their state-level consumer privacy laws for any data they collect and maintain. This involves a data mapping process to identify the collection, use, and disclosure of any regulated personal information, such as consumer information collected from the organization's website or job applications.

Then, organizations will need to implement the requirements of the laws concerning an individual's personal information. This includes providing the requisite public-facing privacy notices; giving individuals the right to access, correct, delete, and limit the sale or sharing of their personal information; and updating contractual arrangements with service providers or contractors who process regulated data on behalf of the organization.

Data sharing regimes

Issue: The interplay between HIPAA and other patient privacy laws and mandatory data sharing regimes, such as California's Data Exchange Framework (DxF).

Question for HIPAA compliance officers: What should HIPAA compliance officers know about the DxF and similar state frameworks?

Frey's advice: For context, California Assembly Bill 133, which Governor Gavin Newsom signed into law in 2021, enacted California Health and Safety Code Section 130290 and placed California on the path to building the statewide DxF. This includes a single data sharing agreement (DSA) and a common set of policies and procedures (P&Ps) that govern and mandate "real-time" access to or exchange of health information.

The DxF is "technology agnostic," which means participants only need to share health information with other participants through an existing exchange network, health information organization, or other technology as long as it adheres to specified standards and policies.

This is the first time California has focused efforts on implementing a statewide data-sharing network and making participation mandatory among most health plans and healthcare providers in the state (including small physician organizations).

Mandated participants must execute the DSA by January 1, 2023, and begin sharing what is called “Health and Social Services Information” for treatment, payment, and healthcare operations over the DxF by January 1, 2024.

CalHHS adopted the DxF in July 2022 and released the final versions of the DSA and initial set of P&Ps after a year of development. This release contained the bulk of guidance, technical specifications, and processes to support the DSA and addressed the purposes and requirements for information exchange, breach notification, privacy and security safeguards, data elements, and a patient’s right to access.

Some data obligations imposed on participants—such as the DSA’s breach notification requirements—are inconsistent with HIPAA and other state privacy laws, ultimately creating complexities for participants navigating health privacy and security requirements.

Organizations subject to compliance with the DxF must assess its impact on their policies and procedures, particularly regarding privacy and information security compliance and their electronic health record-sharing practices.

Impact of Meta lawsuit

Issue: A lawsuit recently filed in the Northern District of California alleging that certain U.S. hospitals violated HIPAA by providing Meta (Facebook) with sensitive patient information without permission.

Question for HIPAA compliance officers: Tell us more about how the organizations charged with HIPAA compliance could have done better. What is the overall message other HIPAA CEs should take from this lawsuit?

Frey’s advice: A complaint that stems from a report released by The Markup/STAT found that among *Newsweek*’s top 100 U.S. hospitals, over a third used the Meta Pixel tracking tool on their websites, which collected patients’ health information when they visited the hospitals’ sites. For example, when scheduling an appointment, a patient would need to enter the underlying medical reasons for booking the appointment.

The complaint alleges that the plaintiff and class members had their sensitive health information shared with Meta/Facebook without their consent or knowledge, prompting Facebook to send targeted ads relating to their medical condition. The lawsuit alleges various legal theories, including violations of the CMIA—which is California’s analog to HIPAA—and the state’s constitutional right to privacy (excluding HIPAA since it does not provide a private right of action).

This case should serve as a warning to healthcare providers using similar cookie and tracking technologies on their websites. It demonstrates the challenges providers face with appropriately safeguarding protected health information (PHI) collected on public-facing websites and within patient portals.

Sensitive health information and state vs. HIPAA regulations

Issue: The application of provider obligations under HIPAA and potential conflict with state laws relating to the disclosure of certain sensitive health information, such as reproductive healthcare or gender-affirming care.

Question for HIPAA compliance officers: Can you give a brief overview about what HIPAA compliance officers need to know?

Frey’s advice: Following the Supreme Court’s decision on *Dobbs v. Jackson Women’s Health Organization* that overturned *Roe v. Wade,* which permits the constitutional right to an abortion, state legislatures became authorized to regulate abortion. As a result, states enacted a patchwork of laws, including laws that prohibit access to abortion and related reproductive health services.

To enforce these restrictive laws, state prosecutors and law enforcement agencies will likely turn to patient medical records and related healthcare information in the search for evidence of potential civil and criminal violations, raising questions about whether existing health information privacy laws sufficiently protect both patients and healthcare providers.

Although HIPAA and state health privacy laws provide broad protection for patients regarding when and how their providers may use and share medical information, these laws are far from absolute protection and are often limited in their application.

HIPAA may not prohibit certain disclosures without authorization from the patient. State laws that support criminal or civil action against those seeking or facilitating an abortion may be used as the basis for a permissive disclosure of PHI “for law enforcement purposes” by compelling providers and CEs to disclose abortion-related PHI to law enforcement and state officials.

As a result, some states enacted laws that enhance privacy protections around the medical information of those seeking abortions, such as California’s Assembly Bill 2091. This bill aims to strengthen privacy protections under the CMIA for medical records related to abortion care by prohibiting disclosures to law enforcement and out-of-state parties seeking to enforce abortion bans in other states.

These new legislative measures raise complex legal questions and could push some providers and companies to choose between complying with California law and another state’s mandate to disclose information in response to a warrant or other legal processes

in an abortion-related investigation. Ultimately, such clashes will not be easily resolved and might require clarity from courts following constitutional challenges (particularly under the Constitution's Full Faith and Credit Clause).