

Report on Patient Privacy Volume 24, Number 3. March 07, 2024 As AI, Interoperability Concerns, Collaboration Imperative Increase, 'This Is Privacy's Year'

By Jane Anderson

Health care organizations are increasingly relying heavily on their privacy departments not only for issues involving HIPAA, but also for key consultations on new state statutes, vendor management and data that's not protected health information (PHI), a group of privacy and compliance officers said.

In fact, privacy now has an early seat at the table for multiple significant discussions, and health care entities are integrating the department into higher-level work groups, they said Feb. 27 in a session at the 2024 National HIPAA Summit.

"For years, I feel like I've been saying, 'This is privacy's year. This is where it's in front of all these people. This is going to be when it's on the tip of everybody's tongue.' But I truly believe it's arrived," Lauren Groebe, Baxter International Inc. associate general counsel for privacy, cybersecurity and digital, told attendees.^[1]

The flurry of new state privacy laws—plus the rules on online tracking technologies and the sophistication of vendors using data and data rights—means that "I think privacy's time has arrived, and therefore, our visibility inside of our organizations is as important as it ever was," Groebe said.

Two topics have remained "front and center" for the last several months, Groebe said: new state privacy legislation and HHS Office for Civil Rights (OCR) guidance on online tracking technologies.

On state privacy legislation, Groebe noted that health care organizations are often "mostly exempt from these state laws. However, you still have to look at these [laws] pretty closely to ensure that consumer personal information you may have that's not PHI isn't otherwise regulated." Baxter International has been tracking these new state statutes carefully "to ensure nothing's falling through the cracks," Groebe said.

Baxter has also been working to ensure it is complying with OCR's pixel guidance as it applies to its websites and its apps, she said.

Katie Gorris, chief privacy officer and compliance director at Intermountain Health, told attendees she has also been following developments in artificial intelligence (AI), coupled with rapidly evolving technology. "It's an area where we are thinking about both data protections and responsible use," she said. In addition, Gorris said her team has been concerned about security and potential data breach incidents by vendors and business associates (BAs).

Mary Beth Ireland, compliance consultant at Inova Health System, said her team "spends a fair amount of time" talking through data interoperability issues, data sharing with patients and dispelling those patients' ideas surrounding medical records.

This document is only available to subscribers. Please log in or purchase access.

[Purchase Login](#)
