Healthcare IT News

Health systems' websites still face uncertain regulatory terrain

After a federal court ruled that healthcare organizations sharing individual IP addresses with third parties did not constitute a HIPAA breach, legal ambiguity remains, says one privacy expert.

October 8, 2024
By Andrea Fox

Data collected on providers' unauthenticated websites and shared with third parties is still a liability from regulatory agencies and a potential cause for class action litigation, says Iliana Peters, an attorney and shareholder at the legal firm Polsinelli.

Wide scope of third-party data

The battle over hospital online data tracking has been going on for the past two years, since a Baltimore patient filed a class-action suit against Facebook parent company Meta Platforms, alleging that it was using tracking tools to access patient information from health system websites and portals for targeted marketing.

Since then, politicians have held hearings on Capitol Hill. The U.S. Department of Health and Human Services crafted new tracking rules. The American Hospital Association has pushed back and filed suit. Most recently, the HHS undertook – and then quickly dropped – an appeal in AHA v. Becerra that sought to bar enforcement of the Office for Civil Rights rule governing the use of online-tracking tools.

What comes next is uncertain, but healthcare entities still face a significant burden, says Peters – and they must stay on top of how their tools can leave them vulnerable to costly lawsuits and civil penalties. "They [don't] realize the scope of data that is collected by these third-party entities," Peters said.

One study released earlier this year found that sharing hospital website user data with third parties is common. Provider privacy policies examined in the study were largely inadequate in how they disclosed the use of third-party tracking technologies to consumers.

This past summer, after HHS dropped its AHA v. Becerra suit, the hospital group cheered the fact that health systems can "safely share reliable, accurate healthcare information with the communities they serve without the fear of federal civil and criminal penalties."

But Peters says questions remain regarding the use of other tools like appointment scheduling, geolocation features, translation tools and chatbots on unauthenticated websites.

"Other activity, arguably, would be in scope because the ruling doesn't say it's not," she explained. "The state law requirements are all still at issue, and in some cases are more stringent than HIPAA. So frankly, this really didn't change much."

"You still have to take steps to protect data," she said.

Trolling in gray areas

Peters, once OCR's acting deputy director for the data privacy and security program at the end of a 12-year tenure with HHS, said HHS has opened more than 100 cases associated with this activity under HIPAA while states and the Federal Trade Commission have also launched multimillion-dollar lawsuits.

The highest risk is class action litigation.

"We are seeing hundreds of thousands of lawsuits associated with these activities and class action litigation demands from plaintiffs' attorneys," she said.

They are trolling healthcare websites with publicly available cookie trackers.

"Anyone can get one."

They then review the entities' terms of use disclosures in their online privacy policies to see if those activities are discussed, if consent is obtained and if other applicable legal requirements are met.

"Several of our clients have had multiple demand letters for multiple thousands of dollars from multiple different plaintiffs' attorneys in this respect," Peters said.

"It's really the Wild West right now, and plaintiff's attorneys are taking full advantage of the lack of good case law here."

Providers must remain risk-averse

Understanding all the data that third-party tools collect and use and following all regulatory requirements for consent and use of data can be a heavy lift, especially for those dealing with requirements across multiple states and all different types of data, Peters said.

While the policy is not clear on data collected on public websites, it's not clear "why all of this protection is necessary for data when it's very likely that the individual who is the subject of that data doesn't expect that data to be protected."

The tough part for healthcare organizations "is that they have a mission and they need to meet their patients where they live in the language that they prefer with services that are easy to find," she said.

They can't do it because many of the vendors who do translation services and mapping services will not sign business associate agreements. But there's a lot of confusion because a lot of the data in question, according to HIPAA, can be put on a postcard and sent in the mail for all to see, she noted.

"It's like trying to reconcile an electronic postcard equivalent."