HIPAA REGULATORY ALERT

CUTTING-EDGE INFORMATION ON PRIVACY REGULATIONS

Tracking Software Can Lead to HIPAA Violations

The HHS Office for Civil Rights (OCR) has released a bulletin warning the use of website tracking technologies could result in HIPAA violations. Covered entities need to review their use of these tracking technologies and make necessary improvements.

OCR explained regulated entities are "not permitted to use tracking technologies in a manner that would result in impermissible disclosures of protected health information (PHI) to tracking technology vendors or any other violations of the HIPAA rules."

The bulletin specified some commonly used website technology OCR said can lead to the disclosure of identifiable patient information protected under HIPAA. *(The bulletin is available online at: https://bit.ly/3kM5elZ.)*

Healthcare organizations make broad use of website tracking technologies, says **Kimberly Castellino Metzger**, JD, partner with McCarter & English in Indianapolis.

"Healthcare organizations and other HIPAA-covered entities and their business associates have been using these tracking technologies for a variety of purposes to improve the patient experience, but also for things like marketing, to gather information about people who visit their site, and use their apps for marketing purposes," Metzger explains. "The bulletin is primarily talking about not necessarily tracking technologies used by the covered entity — although they can certainly be covered as well — but these are mostly vendors who use tracking technology on behalf of the covered entity."

Metzger recommends organization conduct a mapping exercise so leaders understand what tracking technologies are in use and where. It is important to understand the difference between unauthenticated and authenticated pages.

Pages in which a user must enter login credentials or buying information to gain access — like the patient portal — are authenticated sites, whereas the main website page that introduces the organization might be unauthenticated, Metzger explains. The authenticated page is more likely to contain PHI because identifying information must be entered to access the page.

But the guidance makes clear unauthenticated pages also can contain PHI. The regulators are looking at whether a person may be identifiable through an IP address simply by connecting to the website.

"If you have XYZ HIV clinic, and you're on that page looking around trying to find a provider, then it can be reasonably inferred that you have a concern about HIV — something that's considered pretty sensitive," Metzger explains. "You don't necessarily have to have an existing treatment relationship with the provider. You don't necessarily have to provide your name, address, telephone number, healthcare information, things like that, to be considered PHI."

Covered entities should not define PHI too narrowly for these purposes, Metzger cautions. A healthcare organization may be disclosing PHI to vendors of tracking technology even without giving them direct health-related information about an identified individual.

"If you're just providing the IP address through an identifiable person who goes on the site, it could still be considered a disclosure of PHI to the vendor," Metzger explains. "I also think you need to be very, very careful to have a BAA [business associate agreement] in place."

The use of such tracking technology — especially the potential for PHI transmission — may come as a surprise to many risk managers and compliance officers, says **William P. Dillon**, JD, shareholder with Gunster in Tallahassee, FL.

"I don't think people knew there could potentially be disclosure, because I think if they did know, I can't imagine hospital risk managers or privacy officers and security officers would have ever allowed that to occur," Dillon says. "In my mind, OCR is putting everybody on notice."

Now that OCR has issued this bulletin, the onus is on covered entities to address the issue promptly, Dillon says. OCR preached for years about ensuring patients have appropriate access to their information without delay, and it was not happening.

"Lo and behold, what have we had the last three or four years? We've had their right of access initiative, and we've had all sorts of provider fines levied against people for not adhering to that particular component," Dillon says. "I think the same potential for enforcement is there with this bulletin."

As with so many scenarios in healthcare, the specific use of a tracker will guide an assessment of how the use fits under HIPAA, says **Matthew Fisher**, JD, general counsel for Carium, a telehealth and remote patient-monitoring company based in Petaluma, CA. The guidance from OCR provides some broad strokes, which can be boiled down to a few primary considerations. The considerations include where on a website or in an application the tracker is placed, what information is collected, who can access the information, and where the information is sent.

"From the HIPAA perspective, if information is kept within an organization and not sent outside, it is more likely that a problem will not come up under HIPAA, at least over who has access," Fisher says. "However, if an organization gives anyone else access to the information collected by the tracker, then it is necessary to consider if the collected information qualifies as PHI, and how to get a business associate agreement in place. Those are some of the initial steps, but they help demonstrate the need to be careful."

Beyond the potential interaction with outside organizations, Fisher says before a tracker is deployed, the organization should gain an understanding of how it functions. Does the tracker gather more information than is needed? Who can access the information collected by the tracker? Where is the tracker placed?

"Answering those questions will help identify other questions and guide informed usage," Fisher says. "The ultimate key is to ask questions and go into situations with eyes wide open."

Action Needed

Healthcare organizations that implement web tracking technologies must take care to ensure tracking of user behavior is not tied to personal information, says **Ian Cohen**, CEO of Lokker, a provider of online data privacy and compliance solutions in Redwood City, CA.

Many trackers like Facebook, Medtargetsystems, BlueKai, and ShareThis, as well as session replay scripts like Crazy Egg, LogRocket, and Microsoft Clarity, enable website owners to configure the tracking script to prevent incidental collection of personal information, Cohen explains. For safety — and to shield PHI — these trackers should not be included on webpages that use forms to collect personal information and should not use identifiers that can enable third parties to re-identify an otherwise anonymous visitor.

Understanding if PHI is at risk by a website tracking technology requires somewhat sophisticated knowledge of how the tracker is configured and analysis of the "payload" of what user data is transmitted from each page. Cohen says marketing teams that plan to implement these tools for understanding website usage, and wish to retarget visitors, need to address these issues:

- Is the tool configurable as to not collect sensitive information?
- Can the tool be effectively deployed without including it on pages with web forms that capture personal information?
- Does the technology create a user/session ID that can later be used (by a data broker or customer data platform provider) to re-identify the visitor?

"The first step for healthcare providers is to ensure they know exactly which trackers and cookies are currently implemented on their websites," Cohen says. "With a complete inventory, the marketing, IT, and privacy teams can evaluate the function and business needs of these third-party providers. Next, ensure that the privacy policy and website consent management tools appropriately reflect the tools in use on the site, and provide HIPAA-compliant descriptions of the information to be used and its specific purpose."

On implementation, marketing/web teams need to properly configure the trackers to avoid collection of sensitive data. This is usually a combination of setting the tracking codes properly as well as managing deployment of these trackers via their tag management system, Cohen explains.

Brad Rostolsky, JD, partner with Reed Smith in Philadelphia, suspects that because the use of tracking technology by vendors has become more prevalent, OCR believed it would be useful to remind everyone HIPAA applies to these relationships.

"Ultimately, most of the guidance really just serves as a reminder that if a covered entity engages a vendor, and that vendor has access

to PHI, then the vendor is a business associate and needs to sign a business associate agreement," Rostolsky says. "This does not reflect a change in approach."

OCR's discussion about unauthenticated webpages may be better served with some follow-up discussion, Rostolsky says. Although OCR acknowledged these webpages "generally do not have access to individuals' PHI," it also noted all individually identifiable health information "collected on a regulated entity's website or mobile app generally is PHI."

"It seems untenable for OCR to treat public-facing websites that do not require a login by an individual as part and parcel of a regulated entity's PHI repository," Rostolsky says. "Hopefully, we will see some clarifying guidance on this soon." ■

OCR Strengthens Confidentiality of Substance Use Disorder Patient Records

The Office for Civil Rights (OCR) and the Substance Abuse and Mental Health Services Administration (SAMHSA) recently announced proposed changes to the Confidentiality of Substance Use Disorder (SUD) Patient Records under 42 CFR Part 2, which could affect HIPAA compliance programs.

Part 2 protects patient privacy and records concerning treatment related to substance use challenges from unauthorized disclosures. The proposed rule "increases coordination among providers in treatment for substance use challenges and increases protections for patients concerning records disclosure to avoid discrimination in treatment." *(More information on the proposal is available online at: https://bit.ly/3jK1Uro.)*

Currently, Part 2 imposes different requirements for SUD treatment records than the HIPAA Privacy Rule. This can cause confusion among covered entities trying to comply with the rules — and that, in turn, can complicate or denigrate the care provided to SUD patients.

If finalized, the new rule would provide long-awaited relief for Part 2-regulated healthcare providers (and their patients) who have wrestled for years with the inconsistencies across these two federal privacy frameworks, says **Vicki J. Tankle**, JD, partner with Reed Smith in Philadelphia.

"Those providers would need to re-evaluate their health privacy compliance programs that are currently designed to comply with Part 2's far more stringent standards," Tankle said. "While this may cause some operational challenges, and may also frustrate providers who have spent time and financial resources in complying with strict Part 2 requirements, I think consistency across these two frameworks will ultimately enhance information-sharing and care coordination to the benefit of both providers and their patients. It will reduce confusion and compliance challenges for providers currently regulated by these dual standards."

For example, the response to this change in the rule would include streamlining the provider's privacy notice and practices around responding to patient requests for an accounting of disclosures and restrictions on disclosures, Tankle says.

If finalized, the proposed rule would afford Part 2-regulated providers with new flexibility, consistent with HIPAA, around obtaining patient authorization to use and disclose information for treatment, payment, and healthcare operations purposes (TPO).

"In particular, Part 2-regulated providers who are currently required to obtain separate written patient consent for each TPO use or disclosure would be able to obtain a single patient authorization applicable to future uses and disclosures for TPO purposes," Tankle says.

More Ability to Share

The proposed change is driven in part by the improved ability to share information electronically, along with a push for continuity of care and coordination between providers, says **Amy M. Joseph**, JD, partner with Hooper, Lundy & Bookman in Boston.

"This has become more and more of a challenge with insurance types of information, because 42 CFR Part 2 is so strict with how you can use the information," Joseph says. "Under Part 2, you have to have the individual consent. It's a pretty prescriptive requirement right now regarding what that consent must look like."

The proposed rule would create a much easier process to facilitate sharing information for patient care

purposes and for payment purposes — much more streamlined and closer to HIPAA.

"The biggest takeaway on the Part 2 side is that going forward, there's now going to be a proactive requirement to self-report any breaches, like we've always had under HIPAA," Joseph says. "Part 2 has potential criminal enforcement, but we rarely see it enforced, and there's no proactive duty to go to the government or to the individuals to let them know that a breach has occurred. That is the other big change that will come out of these rules."

Advancing Patient Rights

Melissa Soliz, JD, partner with Coppersmith Brockelman in Phoenix, notes Congress passed the Coronavirus Aid, Relief, and Economic Security (CARES) Act in 2020, promising to give individuals suffering from SUDs the same advantages of integrated care afforded to patients suffering from other maladies. The proposed rule changes will fulfill that promise while strengthening HHS' ability to enforce SUD privacy protections and prohibiting discrimination against those suffering from SUDs, she says.

"These proposed regulations are desperately needed as the ranks of those suffering from SUDs continues to swell as the opioid epidemic rages across the country," Soliz says.

The proposed rule changes will advance patient rights by putting the full force of HIPAA notice, complaint, and enforcement structure behind SUD privacy protections, Soliz says. It will do so by requiring SUD treatment providers to self-report breaches of SUD records and by prohibiting the use of SUD records and testimony against SUD patients in a broader range of civil, criminal, and administrative proceedings and law enforcement investigations.

"The proposed rule changes will also afford SUD patients the benefits of better care coordination and treatment by allowing HIPAA-covered healthcare providers and health plans to use and disclose SUD records for any HIPAA-permitted purpose, if the SUD patient has consented to the use and disclosure of their SUD records for treatment, payment, and healthcare operations activities," Soliz says.

Because this is a proposed rule, healthcare organizations do not need to change anything immediately in response to this proposed change, says **J. Malcolm DeVoy**, JD, partner with Holland & Hart in Las Vegas. The final rule may end up different from the proposed rule, as is often the case, once HHS receives comments from stakeholders and industry.

For healthcare providers who do not offer SUD treatment programs, many will not see any changes. For providers who work in coordination with SUD treatment programs, such as psychiatric facilities or practices involved in the care of patients undergoing treatment, these rules will make it easier to share and disclose SUD-related records.

Administrative and clinical staff will need to review their policies and procedures regarding authorizations, sharing, storing, accounting for, and disclosing patient information subject to the protections of Part 2 to understand what uses are permitted as well as which are now prohibited.

These rule changes may affect all practices to some degree, and the entities that do not regularly encounter Part 2 likely will face the most challenges, DeVoy says. Facilities, hospitals, and practices enmeshed with SUD programs will understand the points of contact between the final rule and their practices, and be able to anticipate these changes.

"Practices within infrequent contact with SUD treatment, such as pediatric practices, or practices where SUD treatment may be relevant to other care, such as OB/GYN practices, may struggle and even be caught unaware because of how distant the requirements of Part 2 are from their practices," DeVoy says. "Due to the broader sweep of information that may be protected under Part 2 in the final rule, and the administrative penalties that may attach to violations, any practice that may receive Part 2-protected information needs to be aware of these changes."

Greater Accessibility for Patients

These changes would create greater accessibility for the patient in the treatment continuum, says **Thomas Britton**, MD, CEO of American Addiction Centers in Brentwood, TN.

"Healthcare organizations should review their current health information and information privacy policies to conform them to the changes in the proposed rule, as well as reviewing their consent forms. For non-SUD providers, it will be necessary to review how the data are physically maintained and segmented in the electronic health record to ensure that adequate safeguards are maintained under the proposed rule," Britton says. "They should also review their Notice of Privacy Practices under the HIPAA Privacy Rule, and the expanded proposed prohibitions on use and disclosure of Part 2 records for civil, criminal, and administrative disclosures." ■