After Meta pixel HIPAA gaffe, check your online business associate agreements

by: Roy Edroso

Effective Jul 7, 2022

Published Jul 11, 2022
Last Reviewed Jul 14, 2022

An expose caught major health systems kicking patient data to Meta, Facebook's parent company, via their online appointment page. The exposure of patient data may have you wondering: Are my online services doing the same thing and, if they are, are my business associate agreements (BAA) protecting me?

Data journalists at The Markup, assisted by the medical journal STAT, revealed in a June 16 article that they had found the scheduling features of many big health systems' websites — including those of Mass General Brigham, New York Presbyterian and Duke University hospitals — had a piece of code called the "Meta pixel" that would, without the patient's knowledge, make "an intimate receipt of the appointment request for Facebook," including not only the name and other biographical data for the patient but also "details about their medical conditions, prescriptions and doctor's appointments." The code would then send the data to Facebook, The Markup reports.

The Markup contacted the health systems about this, and many of them removed the Meta pixel — sometimes without saying anything about it.

There is already one lawsuit in progress in California's Northern District Court by an anonymous patient who claimed that use of their information as accessed via the Meta pixel at a MedStar website violated their rights under various laws, including HIPAA and the Electronic Communications Privacy Act of 1986 (ECPA).

This plaintiff is suing Meta, but practices that have or use third-party appointments software may be concerned that this or a similar piece of code may also be violating their patients' privacy — and that, as with any breach of protected health information (PHI), they may be liable to investigation and prosecution under HIPAA by HHS' Office for Civil Rights (OCR), among others.

Experts surprised

Experts expressed surprise that large and presumably HIPAA-astute medical organizations would have the pixel in public-facing pages.

"It's one thing to download an IP address, which also can be considered PHI," says William P. Dillon, an attorney with Gunster in Tallahassee, Fla. "But then to also download information specific to the appointment and even the patient's condition is certainly cause for concern for those hospitals."

Weston L. Hall, a partner with Chamblee Ryan in Dallas, finds it interesting that, according to the story, the systems "could remove the Meta pixel pretty easily after someone discussed it with them. I would hope software makers in the health care space were more likely to have their software HIPAA-compliant [in the first place]."

"I don't understand why a hospital like Mass Brigham or Houston Methodist would do it," Hall adds. "The benefits that they'd be getting out of any of this data-sharing must be far surpassed by the risks they were taking, opening themselves up to not just a few but potentially thousands of HIPAA violations, the penalties for which can be significant."

'Bare bones' BAA not enough

This raises the question of what your BAAs with appointment program vendors should include. As a matter of standard operating policy, you should be reviewing all of your BAAs annually under HIPAA rules as part of your risk assessment duties. But services that take data directly from patients should get extra attention.

Matthew Fisher, general counsel for Carium, a virtual care platform based in Worcester, Mass., reminds you that "not every internet connected service requires a BAA. For example, an ISP [internet service provider] is just transmitting data and never holds onto it. Given the simple act of transmission, an ISP falls into the 'conduit' category and there is actually specific guidance from OCR that an ISP is not a business associate."

But patient forms that are used for appointments are a different story. Experts agrees that vendors such as these should have BAAs that provide a level of protection to the hiring practice in case the vendor breaches PHI (*PBN 7/19/21*). Yet Michael F. Arrigo, managing partner, No World Borders in Newport Beach, Calif., notes this protection is not necessarily

complete — especially when it's a boilerplate, "bare bones" agreement such as you might get from the public website of vendors like ZocDoc.

Even when you sign a BAA with them, such companies "are only business associates when they start disclosing information on behalf of a HIPAA-covered entity," Arrigo says. "If the business associate agreement is prepared by ZocDoc, that's a convenience to their customers and I'm sure it speeds up the sales cycle. But it doesn't protect the covered entity from a breach because ultimately the covered entity is responsible for a breach."

Faisal Khan, senior legal counsel and hospitals and health systems practice lead at Nixon Gwilt Law in Cleveland, reminds you it's the covered entity (CE) and not the business associate (BA) that has the direct/primary liability for a breach under HIPAA. "The provider's defense is that the error was caused by the business associate, but the reporting obligations and potential fines and civil negligence claims filed by patients are all risks directly attributable to the provider," he explains.

Khan also reminds you that "indemnification by a contracted vendor is not a required provision in a BAA under HIPAA," and "even if there is indemnification, it is likely going to be capped at a certain financial threshold."

As a CE, the practice must do its due diligence on the vendor in any case and assure "that [HIPAA-required] policies and procedures are in place," Arrigo says. "They need to understand how the information is being used and disclosed and the uses and disclosures have to be consistent with their notice of privacy practices."

To make sure this has been done, practices should write that understanding into their agreement.

"CEs should ask [the vendor] direct questions, e.g., are you using a Meta pixel? Are there any back doors in your system? Are you connected to social media in any way?" Arrigo says. CEs should get "reasonable assurances" on all of these from the vendor and that the vendor is "maintaining all of your protected health information in a way that prevents unauthorized uses and disclosures," he adds. "Then the covered entity could say [in the event of an issue], 'Look, we relied on that, we asked the questions and that's what they said.'"

Khan suggests you also write the agreement so that when the vendor uses subcontractors, they have to get your approval first. Finally you should ascertain that the vendor "has not been involved in prior HIPAA breaches or other liabilities and, if they have, [they] need to disclose the circumstances of them and the risk mitigation steps they took to ensure that doesn't happen again," Khan adds.

Be cautious of all agreements

Dillon suggests you comb all relevant agreements with the appointment vendor to make sure the data they're moving doesn't go in other directions, and stipulate that it would violate your agreement if it did.

"I'm not super concerned with the vendor utilizing PHI to help the practice perform functions — that's what a business associate is supposed to do," Dillon says. "But are they also allowing that information to be disclosed to other vendors? Does the practice know about [that specific use], about the purpose of it, and whether that vendor is in turn requiring downstream BAAs of its own associates to whom they are disclosing your information — or are they even performing a business associate function?"

Dillon says he's found that vendors nowadays are "really pushing the line as to what they can do with the data" in the BAAs they propose. You shouldn't let that slide — even if they say they want to use only your de-identified patient data. As studies have shown, such data is "not always as de-identified as we think it is," Dillon says, "and may in fact be subject to re-identification" — a process by which de-identified data can be put back together to reveal PHI.

2 more things to watch

- **HIPAA's not the only issue**. Your patients have privacy rights under other laws, including those of your state. In addition to HIPAA and ECPA the California case cites state privacy laws; Dillon notes that in Florida, Chapter 456 of the Sunshine Law requires specific patient consent for marketing communications use.
- **Talk to your vendor**. While your due diligence seems to put you in an adversarial position with your vendors, you should work with them, at least at first, to understand what they're doing. "The vendors I've worked with are very transparent, and if they're asked a question they're good about answering," Hall says. You can then verify what they've told you.

Resources

- The Markup, "Facebook Is Receiving Sensitive Medical Information from Hospital Websites," June 16, 2022: *https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites*
- Complaint, John Doe v. Meta Platforms. Inc., filed June 17, 2022: *https://docs.reclaimthenet.org/Doe-v-Meta-Platforms-FB-Tracking-Pixels.pdf*

BACK TO TOP

Part B News COLLECT EVERY DOLLAR YOUR PRACTICE DESERVES

Part B News

- PBN Current Issue
- PBN User Tools
- PBN Benchmarks
- Ask a PBN Expert
- NPP Report Archive
- Part B News Archive

Coding References

- E&M Guidelines
- HCPCS
- CCI Policy Manual
- Fee Schedules
- Medicare Transmittals

Policy References

- Medicare Manual
  - 100-01
  - 100-02
  - 100-03
  - 100-04

Subscribe | Log In | FAQ | CEUs Part B Answers Select Coder

Join our community!

Like us on Facebook

Follow us on Twitter

Join us on LinkedIn

Read and comment on the PBN Editors' Blog

Contact the Part B News Editors

H3.Group a SimplifyCompliance business Our Story | Terms of Use & Privacy Policy | © 2022 H3.Group