COSMOS
Navigate the Compliance Universe

Compliance Today - April 2024

Alisa Lewis (alewis@carequest.org, linkedin.com/in/alisa-lewis-chc-crisc/) is the Governance, Risk, and Compliance Director at CareQuest Institute for Oral Health Inc. in Boston, MA.

Compliance considerations for website tracking technologies

by Alisa Lewis, CHC, CRISC

Many of you may have seen the December 2022 bulletin issued by the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) reminding regulated entities they are "not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI [protected health information] to tracking technology vendors or any other violations of the HIPAA Rules."[1] In July 2023, the Federal Trade Commission (FTC) and OCR issued a joint warning letter to 130 hospital systems and telehealth providers alerting them to the risks of using website tracking technologies.[2] The bulletin and warning letters may have prompted you to examine if your websites shared PHI with any third parties and ensure appropriate controls were in place, such as executing business associate agreements. While there is an open lawsuit filed by the American Hospital Association (AHA) and other health systems in November 2023 disputing the rule promulgated by the OCR bulletin because it is "flawed as a matter of law, deficient as a matter of administrative process, and harmful as a matter of policy," healthcare organizations should not ignore the risks associated with the use of such technology.[3] Even if the court finds in AHA's favor, the risk of using tracking technologies is not only associated with a potential HIPAA violation but also the risk of class-action lawsuits and complaints for violating state and other federal laws.

In the past few years, there has been an increase in settlements and litigation against organizations that should prompt you to further examine the use of website tracking technologies and ensure your organization is appropriately mitigating related risks. The cases have involved complaints of both healthcare and nonhealthcare-related entities and have involved a variety of allegations, such as violations of wiretapping and electronic eavesdropping,[4] the FTC Act,[5] the Video Privacy Protection Act,[6] the California Consumer Privacy Act (CCPA)[7] and other states' privacy laws, and invasion of privacy under common law. As new consumer privacy laws are passed, the potential for violations could expand. Responding to and defending against such complaints can be costly and have a negative impact on your organization's reputation.

As a compliance professional, it's important that you understand what tracking technologies are, potential compliance and legal risks related to the use of tracking technologies, and how to protect your organization against such risks.

Understanding tracking technologies

Various forms of these technologies have been subject to litigation and complaints, including, among others, cookies, tracking pixels, chatbots, and software development kits (SDK), which are often known as devkits. These technologies offer different uses and certain risks.

You may be most familiar with cookies. Cookies are small pieces of data stored in your browser. They are used to identify your device in the future, collect information about the pages you view and your activities on the site, enable the site to recognize you, offer you an online shopping cart, keep track of your preferences if you revisit the website, customize your browsing experience, and deliver ads targeted to you. There are various types of cookies, some of which pose greater compliance concerns than others. First-party cookies are stored on the website you're visiting. Third-party cookies are transmitted to a third-party website and would pose a greater risk of being the subject of a class-action lawsuit or complaint. Single-session cookies help with navigation on the website, only record information temporarily, and are erased when the user quits the session or closes the browser; they are enabled by default to provide the smoothest navigation experience possible. Persistent/multisession cookies remain on your computer and record information every time you visit websites; they are stored on the hard drive of your computer until you manually delete them from a browser folder or until they expire, which can be months or years after they were placed on your computer. Under the current OCR bulletin directive, third-party cookies that are shared with third parties could result in a HIPAA violation if the cookies share PHI. Use of third-party cookies could also result in complaints, such as seen in the complaint against Sephora in 2022.[8]

Tracking pixels are small pieces of code or images on a website that allow the website administrator to track user behavior and interactions. One of the more familiar tracking pixels is the Meta Pixel. On Meta's website, it advertises that the Meta Pixel "can help you better understand the effectiveness of your advertising and the actions people take on your site, like visiting a page or adding an item to their cart. You'll also be able to see when customers took an action after seeing your ad on Facebook and Instagram, which can help you with retargeting."[9] There are several types of tracking pixels, such as conversion pixels, impression pixels, retargeting pixels, and click-tracking pixels.[10]

An SDK is a set of platform-specific building tools provided usually by the manufacturer of a hardware system, operating system, or programming language that includes tools like debuggers, compilers, profiles, code samples, and libraries to create code that runs on a specific platform, operating system, or programming language. App developers, publishers, and other companies use SDKs to integrate their apps with the SDK provider's services. To use an SDK, a company signs a license agreement and embeds the code offered by the SDK provider in their app environment. An SDK has various uses, such as helping a company evaluate data within their app for purposes of improving user engagement or debugging or addressing errors, allowing a company to offer advanced features to users, such as the ability to log in to the app using their social media log in, and it can be used for monetization purposes, including content personalization and targeted advertising. Some SDK providers offer a single SDK that can be used for all these purposes.[11] SDKs differ from cookies because they cannot be removed from the website.

Chatbots are another technology that can result in sharing information with third parties. This technology may not be considered a tracking technology; however, using chatbots could result in compliance issues if not properly disclosed or if you have not correctly contracted with the entity. Chatbots are computer programs that simulate conversations with human users. They may use artificial intelligence, such as natural language processing. Chatbots are an on-demand service for website visitors, making it easier for users to get the information they want.

Compliance and legal risks

Compliance professionals must not only consider risks related to HIPAA noncompliance but must also consider risks related to noncompliance with other laws and regulations that may be affected by website tracking technologies. Recent complaints and class-action lawsuits have included allegations of federal and state law

violations. Reviewing the cases can increase your understanding of your organization's compliance risks. These cases typically involve website tracking technology where a third party intercepts or receives communication between the website operator and the consumer. FTC complaints have alleged violations of unfair and deceptive practices.[12] Class-action lawsuits have alleged violations of various laws, including wiretapping and electronic eavesdropping, Video Privacy Protection Act (VPPA), impermissible uses and disclosures under HIPAA, and invasion of privacy, to name a few.

- **Wiretapping and electronic eavesdropping** – Federal and state laws prohibit wiretapping and electronic eavesdropping, which generally is recording or listening to a conversation between two people where one of the parties is unaware. The basis of these laws can be found in *Katz vs. the United States*, in which the U.S. Supreme Court found that eavesdropping on a telephone call violated a person's Fourth Amendment right against unreasonable searches and seizures.[13] The Court's opinion was that the Fourth Amendment protects people and not places. Litigation and complaints against website operators for wiretapping and electronic eavesdropping violations are more likely to occur in states requiring two-party consent to be recorded.

- **VPPA** – The VPPA, enacted in 1998, protects against wrongful disclosure of personally identifiable information (PII) of consumers that rent, purchase, or subscribe to a video tape service provider.[14] A video tape service provider is an entity that rents, sells, or delivers prerecorded audiovisual material. In recent years, dozens of VPPA class actions have been filed against websites offering online videos and using third-party-tracking technologies. The plaintiffs in these suits argue that websites that offer video content and then share viewers' PII with a third party without the viewers' consent violate the VPPA. This litigation has had mixed outcomes, and more litigation is expected.

- **Invasion of privacy (common law)** – In general, an invasion of privacy is a common law right within some jurisdictions. As seen in *Popa vs. Harriet Carter Gifts* and other suits, plaintiffs allege third-party tracking technologies invade the plaintiff's privacy by sharing their personal information with third parties without consent.

How to protect your organization

Website tracking technology risk assessment

The first step in identifying tracking technology risks facing your organization is to perform a risk assessment of the use of tracking technologies on your websites and vendor websites. The assessment should consider all sites accessed by users external to your organization, including subdomains. During this assessment, key steps to consider include:

1. Identify the individual or department that manages your organization's website. Ask them questions, such as, "Do we use pixels? What information is tracked? Are pixels used to target advertisements to website users? Is video viewing history shared with third parties (violation of VPPA)? Are chatbots used? Is session replay technology used? Is technology used that intercepts communication between a website user and the website? Are 'GET' requests sent to third parties?" ("'GET' is used to request data from a specified resource.")
2. Identify federal and state laws and regulations that impact your organization.
3. Perform a scan of your website to identify what tracking technologies are used.
4. Review existing business associate agreements or other written agreements to identify what contractual

requirements are in place for the third parties to protect PII that is shared through the tracking technologies.

5. Review your website's privacy statement to ensure it complies with state and federal laws about sharing personal information.
6. Review current change management processes that apply to your organization's website. When assessing the change management process, confirm that changes to the website are a part of the existing change management process or have their own change management process.
7. Review the privacy impact assessment process to ensure it is appropriately designed to identify and mitigate risks related to the organization's website.
8. Identify if there are plans to implement tracking technologies.

Once you've identified your organization's risks, you should incorporate mitigating controls within the compliance or privacy programs to address these risks.

Effective privacy program

Having an effective privacy program in place is another way to help protect your organization from risks related to website tracking technologies. I have both compliance program and privacy program implementation and management responsibilities in my current and past roles. With this dual responsibility, I have utilized the seven elements of an effective compliance program in designing an effective privacy program. For organizations with separate compliance and privacy teams, the compliance professional's expertise in establishing and maintaining an effective compliance program can be shared with the privacy officer to help design an appropriate one.

Written policies, procedures, and standards

As with a compliance program, a privacy program should have documented policies and procedures to establish standards and processes to appropriately safeguard personal information. The program should be documented and annually approved by the board of directors or a senior officer if a board does not exist. Specific to information gathered through consumer interactions with websites, a privacy program should have policies, procedures, and technical controls in place (1) to inventory PII in the organization's control and delete the information when it's no longer reasonably necessary to maintain, (2) to prevent collection, maintenance, use, or disclosure or provision of access to PII inconsistent with the organization's representations to consumers, and (3) for access controls to PII. A data retention policy should also be in place.[15]

Sufficient privacy statement and related controls

Under regulations such as General Data Protection Regulation (GDPR) and CCPA, websites have privacy statement requirements related to collecting and using a consumer's personal information. While not all organizations are required to comply with these regulations, they can be utilized as best practices in developing a website's privacy statement. Additionally, organizations can use federal guidance, such as Office of Management and Budget (OMB) memorandum M-10-22, under "Principles for Federal Agency Use of Web Measurement and Customization Technologies."[16] Having a sufficient privacy statement on your organization's website may help protect your organization from the risk of sharing personal information through website tracking technologies. Best practices for website privacy statements related to the use of website tracking technology include:

1. "the purpose of the web measurement and/or customization technology;

2. "the usage Tier, session type, technology used;
3. "the nature of the information collected;
4. "the purpose and use of the information;
5. "whether and to whom the information will be disclosed;
6. "the privacy safeguards applied to the information;
7. "the data retention policy for the information;
8. "whether the technology is enabled by default or not and why;
9. "how to opt-out of the web measurement and/or customization technology;
10. "statement that opting-out still permits users to access comparable information or services; and
11. "the identities of all third-party vendors involved in the measurement and customization process."[17]

If your organization is not required to comply with website statement requirements, the organization will need to determine—using the website risk assessment results—what provisions should be included within the website's privacy statement and what additional controls should be in place. Should you offer opt-in or opt-out? The CCPA requires websites to allow users to opt out of data collection, while regulations such as GDPR require users to opt in. Which options are best for your organization and offer the best protection against risks? How long will you retain the data collected? Do you have appropriate controls implemented to fulfill the provisions in the privacy statement, such as the ability to delete and amend data?

Privacy program leadership and oversight

Organizations should designate a qualified privacy officer who directly reports to an executive responsible for the privacy program, such as the CEO or chief compliance officer. The privacy officer should keep the executive and the board of directors informed of the program as well as any privacy risks facing the organization. The privacy officer is also responsible for ensuring appropriate policies and procedures are documented and the safeguards are designed to effectively protect PII held by the organization.

Training and education

An annual privacy training program should be developed, maintained, and updated to address the privacy risks within the organization. It's imperative for HIPAA-regulated entities to not only perform training required under HIPAA but also training for protecting other PII the organization may track and monitor through its websites. Training should be developed to specifically address website tracking technologies and be provided to those employees based on their roles and responsibilities.

Continuously monitor, audit, and evaluate the program

Periodically, website scans should be performed to identify and confirm website tracking technologies are in place on the site. During periodic risk assessments, website tracking technologies may need to be reassessed. Change management processes should be continuously monitored and audited to ensure website changes are appropriately assessed for compliance and privacy risks and properly approved. As with a compliance program, reviewing and adjusting the privacy program based on assessment outcomes, material events, and/or

organizational changes is essential.

Conclusion

With increasing complaints and class-action lawsuits, OCR and FTC warning letters, and an increase in state privacy laws, compliance professionals should examine their organization's use of website tracking technologies and stay up to date on laws and regulations that may impact the use of such technologies. Reviewing prior settlements and class-action lawsuit complaints can give insight into how your organization may be affected if such technology is used. Compliance professionals should work closely with the privacy team to understand website tracking technology risks, how the risks impact your organization, and how to protect the organization against such risks.

Takeaways

- Compliance professionals must stay informed of litigation and complaints about website tracking technologies and their outcomes.
- State and federal laws should be considered to ensure organizations have appropriate controls in place to ensure compliance.
- A risk assessment should be performed to understand what risk an organization is exposed to through website tracking technologies.
- An appropriately designed privacy program incorporating website tracking technology controls will help mitigate risk.
- Having a sufficient privacy statement on your organization's website may help protect your organization from website-tracking technology risks.

1 U.S. Department of Health and Human Services, "Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates," last reviewed December 1, 2022, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.
2 Federal Trade Commission, "FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies," news release, July 20, 2023, https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking.
3 American Hospital Association; Texas Hospital Association; Texas Health Resources; United Regional Health Care System v. Rainer (N.D. Tex. Fort Worth Division, Nov. 2, 2023), https://www.aha.org/system/files/media/file/2023/11/Case-Complaint-AHA-THA-THR-United-Health-Care-System-v-Rainer.pdf.
4 Popa vs. Harriet Carter Gifts, Inc, No. 21-2203 (3rd Cir. Oct. 18, 2022), https://caselaw.findlaw.com/court/us-3rd-circuit/1970656.html.
5 BetterHelp, Inc., In the Matter of, "Decision and Order," No. C-4796, July 7, 2023, https://www.ftc.gov/system/files/ftc_gov/pdf/2023169betterhelpfinalorder.pdf.
6 Aldo M. Leiva and Alexander F. Koskey, "VPPA Claims Are on the Rise – Latest Trend in Consumer Privacy Class Action Litigation," Baker Donelson, March 13, 2023, https://www.bakerdonelson.com/vppa-claims-are-on-the-rise-latest-trend-in-consumer-privacy-class-action-litigation.
7 Popa vs. Harriet Carter Gifts, Inc.
8 The People of the State of California v. Sephora USA, Inc (Super. Ct. Calif., County of San Francisco Aug. 24,

2022).
9 Meta, "What is the Metal Pixel?" accessed January 30, 2024, https://www.facebook.com/business/tools/meta-pixel.
10 Arslan Jadoon, "What is a Tracking Pixel and How Does it Work?" Replug (blog), May 31, 2023, https://blog.replug.io/what-is-a-tracking-pixel-and-how-does-it-work.
11 Daniel Goldberg and Rick Borden, "Regulators and Litigators are Investigating Data Flows Through SDKs – An Overview and Practical Steps to Reduce Risk," *Technology Law Updates* (blog), Frankfurt Kurnit Klein + Selz, August 23, 2023, https://technologylaw.fkks.com/post/102imku/regulators-and-litigators-are-investigating-data-flows-through-sdks-an-overview.
12 BetterHelp, Inc., In the Matter of, "Decision and Order."
13 Katz v. United States 389 U.S. 347 (1967).
14 18 U.S.C. § 2710.
15 BetterHelp, Inc., In the Matter of, "Decision and Order."
16 Peter R. Orszag, "Guidance for Online Use of Web Measurement and Customization Technologies," Executive Office of the President Office of Management and Budget, June 25, 2010, https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/memoranda_2010/m10-22.pdf.
17 Peter R. Orszag, "Guidance for Online Use of Web Measurement and Customization Technologies."