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.