PULLMAN &COMLEY

Vox Article on Vulnerabilities of COVID-19 Testing Registration System Serves as Reminder of the Dangers of Tracking Tech on HIPAA Covered Entity Websites

Connecticut Health Law

09.22.2021
By Russell Anderson

In 2018, we published an article on Walgreens' use of session replay scripts and how such use could lead to an accidental data breach under HIPAA. Last week, an article in Vox explained how Walgreens was again apparently leaking HIPAA protected-health information on its website through its COVID-19 testing registration system. The story serves as a good reminder that covered entities that use their websites to collect or post patient information need to be especially careful about how their websites are structured and the analytics tools that are used on them.

According to the Vox article, when a user schedules a COVID-19 testing appointment through the pharmacy's site, they are required to complete an online request form which collects basic intake information. After completing the form, the user receives a unique URL confirming their appointment and information contained within the form. The problem with the system, however, is that anyone with the unique URL may access the confirmation page. For example, anyone with access to the individual's browser history (such as a family member or employer if on a work computer), or presumably a well-programmed bot, can obtain the URL link. Once the URL link is found and accessed, the person's PHI is accessible, including not only the date/time/type of COVID-19 testing appointment, but also date of birth, email address, phone number, gender identity and street address.

Further, the site again used data analytics trackers on the testing confirmation pages. The security researchers cited in the Vox article, including Sean O'Brien, the founder of Yale's Privacy Lab, flagged the possibility that the companies that own these trackers — including Adobe, Akamai, Dotomi, Facebook, Google, InMoment, Monetate, as well as any of their data-sharing partners — could be ingesting the patient IDs, which could be used to figure out the URLs of the appointment pages and access the information they hold. As a result, without a business associate agreement and other necessary precautions, the use of these

Vox Article on Vulnerabilities of COVID-19 Testing Registration System Serves as Reminder of the Dangers of Tracking Tech on HIPAA Covered Entity Websites

analytics cookies would likely violate HIPAA.

These two situations serve as a reminder of some dos and don'ts for your healthcare organization's webpage:

1. Do use login credentials (and potentially two-factor authentication) to secure access for any page where PHI is published on your website.
2. Do not use analytics/tracking tools (e.g., cookies) on pages where PHI is collected or posted (at least not without a business associate agreement and a careful review of the tracker's HIPAA compliance). The chance of disclosure to the tracking tool is simply too high.

Please contact Pullman & Comley Health Care attorneys with any questions.

Posted in COVID-19, Privacy

Tags: HIPAA