Risky Business: Using Online Tracking Technologies
January 3, 2023

The U.S. Department of Health & Human Services Office of Civil Rights (OCR) recently issued guidance to HIPAA Covered Entities and Business Associates that use online tracking technologies. While HIPAA Covered Entities may use tracking technologies, that use must comply with HIPAA Privacy, Security, and Breach Notification Rules.

A tracking technology is a script or code on a website or mobile app used to gather information about users as they interact with the website or mobile app. These technologies include cookies, web beacons, tracking pixels, session replay scripts, and fingerprinting scripts. The information these tracking technologies gather can create insights about user activity and improve patient care. Gathered data often includes IP addresses, medical record numbers, home or email addresses, dates of appointments, geographic data, medical device IDs or other unique identifying code—all of which is considered individually identifiable health information.

The OCR guidance clarifies that individually identifiable health information can become protected health information (PHI) when a covered entity collects the data through its website or mobile app when it connects the individual to the covered entity (i.e., it is indicative that the individual has received or will receive healthcare services or benefits from the covered entity). When a covered entity's use of these tracking technologies leads to the collection or disclosure of PHI, the HIPAA Privacy, Security, and Breach Notification Rules apply. Covered entities must ensure they comply with these rules.

Many of these technologies are developed by third-party vendors who can access collected data. These third-party vendors may be considered to provide a service to the covered entity that would, in light of the use and disclosure of PHI, create a direct or downstream business associate relationship. Accordingly, the covered entity must enter a business associate agreement (BAA) with the third-party vendor and meet other requirements under the HIPAA Rules.

All covered entities should:

- Determine if they or their website hosts use tracking technologies,
- Identify what information is gathered and how that information is used,
- Confer with counsel regarding whether the collection and use of information are subject to HIPAA and, if so, are HIPAA compliant, and
- Confirm that they have a BAA in place with all third-party entities tracking any PHI.

Members of GableGotwals' Healthcare Practice Group can discuss any question you might have about:

- The risks and limits of using tracking technologies and related individually identifiable health information in your practice,
- Identifying potential HIPAA and other healthcare regulatory compliance gaps that may result in violations, and
- Ensuring your policies and procedures are comprehensive and up-to-date, including development or review of a BAA.

Philip D. Hixon
phixon@gablelaw.com
918-595-4831

Meagen E.W. Burrows
mburrows@gablelaw.com
918-595-4832

Rhyder M Jolliff
rjolliff@gablelaw.com
918-595-4804