FAQ: Bulletin on Requirements under HIPAA for Online Tracking Technologies

Updated: December 2022

The US Department of Health and Human Services (HHS) Office for Civil Rights (OCR) released a bulletin providing sub-regulatory guidance on requirements for covered entities who use online tracking technologies to follow a user's interaction with a website or application. OCR's bulletin comes on the heels of discussion in the healthcare continuum about the inadvertent transfer of a patient's individually identifiable health information (IIHI) and protected health information (PHI) to the third-party companies that develop and support these tracking technologies.

OCR provided a disclaimer that the contents of the bulletin do not carry the force and effect of law and are not binding. The guidance is only intended to provide clarity to the public.

Key Provisions of the Bulletin:

- Regulated HIPAA covered entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other vendors of the HIPAA rules.
    - **Example:** Disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.
- Individually identifiable health information (IIHI) collected on a regulated entity's website or mobile app generally is considered protected health information (PHI), even if the individual does not have an existing relationship with the HIPAA regulated entity.
    - **Example:** IIHI could include an individual's medical record number, home or email address, dates of appointments, IP address or geographic location, medical device ID, or unique identifying code
- Tracking technologies vendors should be treated as business associates if they are collecting or transmitting information on user-authenticated webpages.
    - **Example:** A tracking technology collecting information about a patient on an authenticated scheduling webpage behind a user login would require a business associate agreement (BAA).
- HIPAA Rules may apply to information captured by a tracking technology on an unauthenticated webpage.
    - **Example:** A tracking technology is deployed on a regulated entity's patient portal login page, registration page, or appointment availability page that collects an individual's login information, registration information, or information on the type of care a patient is seeking.
- Mobile apps that regulated entities offer to individuals are covered by the HIPAA Rules, but mobile apps that individuals voluntarily download that are not developed or offered by or on behalf of regulated entities are not governed by HIPAA Rules.
    - **Example:** HIPAA Rules apply to any PHI collected by a healthcare organizations' mobile app used by patients to track health-related variables, but do not apply to a third-party app a patient chooses to use.
- A HIPAA covered entity is required to follow breach notification requirements if an impermissible disclosure of an individual's PHI is made to a tracking technology vendor that compromises the security or privacy of an individual's PHI.

If you have questions on the above bulletin, please contact the AHIMA Policy & Government Affairs Team at advocacy@ahima.org.