Privacy Regulation of Online Tracking Technologies: Court and Agency Statutory Interpretations and Enforcement Actions

October 24, 2024

Daniel F. Fisher
Digital & Data Legal,
Merck & Co., Inc.

Nancy L. Perkins
Counsel,
Arnold & Porter

Robin Rosen Spector
Attorney
Division of Privacy & Identity Protection,
Federal Trade Commission

Privacy+ Security Forum

U.S. Department of Health and Human Services Guidance on Online Tracking Technologies

- Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates (December '22)
- **Purpose:** To highlight obligations of entities regulated under the HIPAA Privacy, Security, and Breach Notification Rules (*i.e.*, HIPAA "covered entities" and their "business associates") when using online tracking technologies
- **Focus**: "Tracking technologies" -- script or code deployed on a website or mobile app. to gather and share information about a user or user interactions with the site or app
- **Warning**: Use and disclosure of information collected through certain online tracking technologies may violate the HIPAA Privacy and Security Rules where the information is "protected health information" ("PHI")

HHS Views on Online Tracking Technologies

- Insights gained through use of tracking technologies on health-related websites or applications could be used to help improve care or the patient experience.
  - For example, hospitals might use data analytics to determine how many IP addresses accessed webpages providing information about COVID-19 vaccines or treatment in a particular area.
  - This could help the hospitals make decisions about how to allocate their medical and other resources.
- **BUT** this tracking information could also be misused.
- Primary concern is *disclosure of PHI collected through tracking technologies to third parties without individual authorization.*

HHS Guidance: When Is PHI Collected/Shared Through Tracking Technologies?

- Information collected through tracking technologies on a regulated entity's website or mobile app generally is PHI
  - even if the individual does not have an existing relationship with the regulated entity
  - even if the information, such as an IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services.
- If an online tracking technology connects the IP address of a user's device (or other identifying information) with a visit to a webpage addressing specific health conditions or listing health care providers:
  - That combination of information is PHI if the webpage visit relates to the individual's past, present, or future health, health care, or payment for health care.
  - But the IP address together with the webpage visit is "**not a sufficient combination of information to constitute [PHI]** ***if the visit to the webpage is not related to an individual's past, present, or future health, health care, or payment for health care.***"

HHS Guidance: User-Authenticated Websites

- User-authenticated webpages require a user to log in before they are able to access the webpage, *e.g.*:
  - a patient or health plan beneficiary portal
  - a telehealth platform.
- "Tracking technologies on a regulated entity's user-authenticated webpages generally have access to PHI," *e.g.*:
  - an individual's IP address, medical record number, home or email addresses, dates of appointments, or other identifying information that the individual may provide when interacting with the webpage.
  - diagnosis and treatment information
  - prescription information
  - billing information, or other information within the portal.
- "Therefore, a regulated entity must configure any user-authenticated webpages that include tracking technologies to allow such technologies to **only** use and disclose PHI in compliance with the HIPAA Privacy Rule."

HHS Guidance: Unauthenticated Websites

- Tracking technologies on many unauthenticated webpages do not have access to individuals' PHI; in this case, a regulated entity's use of such tracking technologies is *not* regulated by the HIPAA Privacy and Security Rules.
    - "For example, if a student were writing a term paper on the changes in the availability of oncology services before and after the COVID-19 public health emergency, the collection and transmission of information showing that the student visited a hospital's webpage listing the oncology services provided by the hospital would not constitute a disclosure of PHI, even if the information could be used to identify the student."
- **"However**, if an individual were looking at a hospital's webpage listing its oncology services to seek a second opinion on treatment options for their brain tumor, the collection and transmission of the individual's IP address, geographic location, or other identifying information showing their visit to that webpage **is a disclosure of PHI *to the extent that the information is both identifiable and related to the individual's health or future health care***."

American Hospital Assoc. et al. Lawsuit v HHS

- **Claim against HHS:** In 2023, the American Hospital Association and several other hospital groups sued HHS in federal district court in Texas, claiming HHS overstepped its authority in issuing the Guidance.
- **Arguments**:
  - HHS's interpretation of what is "PHI" on an unauthenticated webpage has no legal support.
  - Even assuming the IP address of a visitor to a health-related webpage could reasonably be associated with a particular individual, that could not indicate that individual visited the page ***in connection with his or her own health, health care, or payment for health care***.
    - *E.g.*, "the visit may have occurred due to academic or journalistic research on a heath condition or area provider capacity, general curiosity about something in the news, or just an accidental click on a web link."

American Hospital Ass. Vs. Becerra (Nov. 2023)

- ***American Hospital Association v. Becerra*, -- F. Supp. 3d --, No. 4:23-cv-1110, 2024 WL 3075865 (N.D. Tex. June 20, 2024)**
- **Court Ruling:**
  - HHS lacked authority for the part of its Guidance regarding collection and sharing of PHI via ***unauthenticated*** webpages; that part of the Guidance is vacated.
  - Metadata such as IP address collected on a HIPAA-regulated entity's unauthenticated, public-facing website, does not constitute individually identifiable health information (IIHI).
  - Even if an unauthenticated webpage's metadata could identify a particular individual, "[t]hat information cannot become IIHI based solely on the visitors' subjective motive for visiting the page."
- **HHS Response:** Initially noticed intent to appeal, then withdrew notice of appeal. Currently is "evaluating its next steps in light of that order."

Why Does This Matter? Broader Implications

- *HHS guidance is only 1 piece of a much larger puzzle….*
  - 19+ comprehensive state privacy laws to protect personal and sensitive information
  - Landmark consumer healthcare privacy laws in Washington & Nevada
  - FTC emphasis and intent to protect consumer health data
  - NY State AG commentary on appropriate cookie banners for website data collection

So what is individually identifiable health data?

- Sensitive Personal Information
- Consumer Health Data
- Industry Discussions?

What Are the FTC's View and Priorities?

- **Protection of health/sensitive information**
  - Protecting the privacy of health information: A baker's dozen of takeaways from FTC cases
  - Consumer health information: handle with (extreme) care
  - Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal sharing of highly sensitive data
- **Collecting, Using, or Sharing Consumer Health Information: Look to HIPAA, the FTC Act, and the Health Breach Notification Rule**
  - https://www.ftc.gov/business-guidance/resources/collecting-using-or-sharing-consumer-health-information-look-hipaa-ftc-act-health-breach

Recent FTC Enforcement in Health Data Space

Privacy + Security Forum

- **Monument:** https://www.ftc.gov/news-events/news/press-releases/2024/04/alcohol-addiction-treatment-firm-will-be-banned-disclosing-health-data-advertising-settle-ftc
- **Cerebral:** https://www.ftc.gov/news-events/news/press-releases/2024/04/proposed-ftc-order-will-prohibit-telehealth-firm-cerebral-using-or-disclosing-sensitive-data
- **Easy HealthCare:** https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc
- **BetterHelp**: https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-ban-betterhelp-revealing-consumers-data-including-sensitive-mental-health-information-facebook
- **GoodRx:** https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising
- **FloHealth:** https://www.ftc.gov/news-events/news/press-releases/2021/01/developer-popular-womens-fertility-tracking-app-settles-ftc-allegations-it-misled-consumers-about

Subtleties of Tracking Individual Activity

- **Pixels and other tracking technologies**
  - Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking
- **Anonymization**
  - No, hashing still doesn't make your data anonymous

What Best Practices Should Guide Online Tracking?

- Determine scope of personal information processing and to what extent such processing is needed to meet business objectives
- Decide where to draw your lines in the sand
- Conduct risk assessments
  - Weigh benefits of tracking against risks to consumers
  - Test risk-mitigation measures and remediate deficiencies
- Provide transparency through notices and disclosures
  - Create a robust privacy policy and clearly document decisions
  - Provide notice of data collection before or at the time of collection
- Obtain consent ***prior*** to tracking an individual's website use

Contacting Us

Daniel Fisher

Merck

Daniel.Fisher1@merck.com

Nancy L. Perkins

Arnold & Porter

Nancy.Perkins@ arnoldporter.com

Robin Rosen Spector

Federal Trade Commission

rspector@ftc.gov