MINTZ

Tracking Technologies and Health Information: A Prescription to Avoid Enforcement Action Headaches

May 10, 2023

Presenters

Alea Garbagnati

Head of Privacy

Adaptive Biotechnologies, Corp

agarbagnati@adaptivebiotech.com

- Serves as Privacy Officer at Adaptive
- Leads a team of amazing privacy professionals and provides strategic counsel on privacy compliance, HIPAA, product privacy by design, research, and data strategy
- Has experience in managing privacy topics in the Life Sciences industry in the US and in Europe, particularly in the medical device space
- Serves as an active member of the privacy community – as a member of the IAPP Publication Advisory Board, author of articles on privacy in biotech, member of several industry groups, and a part of the Common Paper Committee

Lara D. Compton

Member

Los Angeles

LDCompton@mintz.com

424.259.4019

- Works at the intersection of health care and technology advising clients regarding compliance with the complex regulatory regime applicable to the use and disclosure of health information
- Advises clients in responding to third party health information privacy and security audits
- Assists clients with health information privacy and security incident investigation and breach reporting under HIPAA and other breach notification laws
- Analyzes risks presented by implementation of new technologies

Kathryn F. Edgerton

Member

Los Angeles

KFEdgerton@mintz.com

424.259.4030

- Trusted advisor to clients ranging from traditional health care providers to disrupter digital health platforms as they navigate the practical and regulatory challenges of health care innovation
- With a focus on addiction treatment and behavioral health, Kathryn has counseled over 100 addiction treatment providers on day-to-day operational needs
- Advises clients on the nuances of HIPAA, HITECH, and state privacy and security laws and regulations, including 42 CFR Part 2, the FTC Act, CMIA, and California breach notification laws

Roadmap

- Heightened Focus on Privacy
- What are Tracking Technologies?
- The FTC's Tracking Technology Concerns
- The FTC's Tracking Technology Enforcement Actions
- U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) Guidance on Tracking Technologies
- State Privacy Law Considerations
- Key Takeaways
- What Does this Mean for the Life Sciences Industry?

Heightened Focus on Privacy

The Heightened Focus on and Evolution of Privacy Law

- Heightened sensitivity regarding privacy of health information following COVID-19 and *Dobbs v. Jackson Women's Health Organization* decision
- Increasing awareness of HIPAA gaps when it comes to privacy of health information
- HHS Office of Civil Rights (OCR) and the Federal Trade Commission have broadly interpreted the applicability of the laws in order to bridge the privacy gaps that exist between HIPAA and other privacy laws
- Continuing efforts to develop more comprehensive federal privacy legislation
- An increasing number of states have enacted comprehensive consumer privacy legislation (which applies to health information, subject to certain exemptions) including **California**, **Colorado**, **Connecticut**, **Indiana, Iowa**, **Utah**, **Virginia …**
- **Washington** just enacted a health information privacy law intended to fill th0 gaps between state law and HIPAA

Slide 5

0 Is it worth mentioning the increased focus on sensitive information in these state laws?
Unknown, 1900-01-01T00:00:00Z

What are Tracking Technologies?

What are Tracking Technologies?

- Tracking technologies involve the use of a script or code (e.g., cookies, tracking pixels and codes, fingerprinting scripts, web beacons) on a website or mobile app to gather information about users as they interact with the website or mobile app
- Pixels are sophisticated snippets of computer code used for tracking users around the web, embedded in the HTML of a website, and work by sending the company that placed the pixel a detailed log of user website interactions
- Cookies are small files that websites send to a user's device that the sites then use to monitor the consumer and remember certain information about them — like what's in a shopping cart on an e-commerce site or login information
- Pixels and cookies can be used together by companies to identify users as they traverse the internet

0

- Tracking technologies are commonly used in advertising to help drive targeted ads (e.g., banner and social media ads), including ads for the products and services of a business with which a user has interacted, as well as products and services from similar businesses

Slide 7

0 Thinking this should be the last line on this slide
Unknown, 1900-01-01T00:00:00Z

The FTC's Tracking Technology Concerns

Federal Trade Commission

Information Privacy and Security Generally

- Generally, the FTC expects that:

  1) Information provided to consumers about the information collected about them and how it will be used and disclosed is accurate; and

  0 2) Companies making representations regarding privacy and security of data will take reasonable steps to secure consumer information

- These obligations extend beyond personally identifiable health information and also apply more broadly to other types of individually identifiable consumer information

- According to the FTC, a sound security plan is built on five key principles:

  - Data mapping
  - Minimum necessary
  - Security safeguards
  - Appropriate disposal
  - Respond to security incidents

Slide 9

0 Is it worth making this even more basic and going for the unfair and deceptive basis of the FTC Act?
Unknown, 1900-01-01T00:00:00Z

Federal Trade Commission

Personal Health Records Breach Rule

- Requires vendors of personal health records (PHR) and related entities to notify consumers and in some cases the media and the FTC following a breach involving unsecured PHR identifiable health information
  - If a service provider to one of these entities has a breach, it must notify the entity, which in turn must provide notice under the Breach Rule
- A PHR is an "electronic record of PHR identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual"
- "PHR identifiable health information" is "individually identifiable health information" (as defined by HIPAA) and, with respect to an individual, information that: (1) is provided by or on behalf of the individual; and (2) that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual

Federal Trade Commission

Personal Health Records Breach Guidance and Health Apps

- The Health Breach Notification Rule does not apply to HIPAA covered entities and their business associates
- Health apps are covered by the Breach Rule if they are capable of drawing information from multiple sources, such as through a combination of consumer inputs and application programming interfaces (APIs) even if some sources do not contain health information
- The FTC provides the following examples:
  - An app that collects information directly from consumers and has the technical capacity to draw information through an API that enables syncing with a consumer's fitness tracker; and
  - A blood sugar monitoring app draws health information only from one source (e.g., a consumer's inputted blood sugar levels), but also takes non-health information from another source (e.g., dates from your phone's calendar)

FTC's Tracking Technology Concerns

- Consumers may not realize that tracking pixels exist because they're invisibly embedded within web pages with which users might interact and may collect (and leak) sensitive data to third parties
- Information collected from a pixel can be used to identify social media profiles and automatically connect a user to the user's social media account creating the potential for interactions that may result in consumer confusion or unwanted sharing
- Hashing personal information to scramble personally identifiable information such as names or email addresses may be inadequate because hashing can be reversed or used to link data across different databases

Slide 12

0 Should we speak to the examples that have been cited in the past year where people booking DR appointments have had information health information sent to FB?
Unknown, 1900-01-01T00:00:00Z

0 0 Then can reference back to it when talking about GoodRX
Unknown, 1900-01-01T00:00:00Z

The FTC's Tracking Technology Enforcement Actions

Recent FTC Tracking Technology Enforcement

Flo Health Allegations Overview

- Flo offered the Flo Period & Ovulation Tracker; its privacy policy indicated that Flo would not share user health details
- Flo shared the information gathered with Google, Facebook, and marketing firm ApplyFlyer without limiting how these entities could use the data
- In 2019, the Wall Street Journal ran a story revealing the data sharing practices
- The FTC brought its complaint in 2020 and finalized its settlement order in June 2021
- This was not brought as a PHR Breach case
- In September 2021, FTC issues its “Statement on Breaches by Health Apps and Other Connected Devices”

Recent FTC Tracking Technology Enforcement

GoodRx Allegations Overview

- GoodRx and Hey Doctor shared medication and health information with Facebook via tracking pixels and other automated trackers in connection with certain URL configurations
- GoodRx shared medication and health condition information with Google and Criteo (a digital advertising company)
- GoodRx used and monetized the personal health information it shared to target GoodRx users with advertisements on the Facebook and Instagram platforms
- Through Facebook's "Ads Manager," a self-serve digital advertising tool, and its "Custom Audiences" ad targeting feature, GoodRx used the information it shared with Facebook to identify its users who had Facebook and Instagram accounts through at least April 2021 on some pages
- These actions were contrary to the privacy policies in place and authorization was not obtained from consumers addressing such additional sharing, violating Section 5(a) of the FTC Act and resulting in a breach requiring notice under 16 C.F.R. §§ 318 et seq. applicable to vendors of "personal health records," but no such notice was provided
- Penalty of $1.5M

Recent FTC Tracking Technology Enforcement

BetterHelp Allegations Overview

- Shared consumers' sensitive mental health information with Facebook, Snapchat, and Pinterest for targeted advertising without contractual limitation
- Disclosed its website visitors' and users' intake questionnaire responses (containing current health status and medical history) as well as email and IP addresses to Facebook for the sole purpose of monetization between August 1, 2017 and December 31, 2020, contrary to privacy policies (violating Section 5 of the FTC Act)
- Failed to implement policies and procedures to ensure practices aligned with privacy statements made to consumers
- Placed a recent college graduate with no marketing experience and little training in charge of deciding which visitor and user information was uploaded to Facebook
- Part of the remedy was $7.8M in partial refunds for customers

Recent FTC Tracking Technology Enforcement

Examples of Problematic Statements/Representations

- Your e-mail is kept strictly private. It is never shared, sold, or disclosed to anyone. Even your counselor won't know your real email address.
- Rest assured, your health information will stay private between you and your counselor.
- We use cookies to help the site function properly, analyze usage, and measure the effectiveness of our ads. We never sell or rent any information you share with us. Read our Privacy Policy to learn more.
- We . . . do not target users with advertising specifying any particular medication based on our data.
- Improperly using HIPAA certification seals

Recent Penalties and Corrective Action Plans

Tracking Technology Highlights

- Prohibited from disclosing identifiable health information (IHI) for advertising, marketing, promoting, offering, offering for sale, or selling any product or service
- Require that third parties that impermissibly received IHI delete all personally identifiable consumer information previously provided, which must be confirmed before any sharing may resume (regardless of whether information is hashed)
- Establish and implement a comprehensive privacy program that protects the privacy, security, availability, confidentiality, and integrity of heath information and meets certain requirements
- Third party privacy assessments initially and every two years thereafter
- Settlement obligations extend for 10-20 years
- Over a million dollars in penalties ($1.5-$7.8 million so far)

Here Comes the Plaintiffs' Bar . . .

An Enforcement Action is Seldom the End of the Story

- Each of these settlements were follow by class action lawsuits
- Causes of action:
  - Breach of implied contract
  - Breach of fiduciary duty of confidentiality
  - Violation of state privacy laws

HHS OCR Guidance on Tracking Technologies

Tracking Technologies and the Definition of PHI

- OCR takes the position that all individually identifiable health information (IIHI) collected on the website or mobile app of an entity subject to HIPAA (Regulated Entity)

> *"generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services"*

- OCR transforms information that many had assumed to be personal information subject to general privacy controls (including a website privacy policy) into individually identifiable health information
- OCR posits that in collecting information through its website, a Regulated Entity "connects" the website visitor to the Regulated Entity and is therefore "indicative that the individual has received or will receive health care services or benefits from the covered entity"

Tracking Technologies on User Authenticated Pages

- An authenticated page is a webpage that requires the user to log in before accessing content and includes provider patient portals, health plan beneficiary portals, and telehealth platforms
- OCR states that generally, tracking technologies on authenticated pages would have access to PHI, such as 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 (which in some cases may include individuals' diagnosis and treatment information, prescription information, billing information, or other information within the portal)
- OCR does not discuss the exceptions to this general rule, nor does the Bulletin provide any actionable guidance regarding proper configuration of authenticated pages using tracking technologies

Tracking Technologies on Unauthenticated Pages

- An unauthenticated page is a webpage that does not require the user to log in before accessing content and may include some provider website landing pages and telehealth platform provider search pages
- OCR takes the position that tracking technologies on Regulated Entities' unauthenticated webpages are collecting PHI in certain cases and that such information is subject to the requirements of HIPAA
  - Login pages of a patient portal or a user registration webpage where an individual creates a login for the patient portal; if the individual enters credential information on that login webpage or enters registration information (e.g., name, email address) on that registration page, such information is PHI that could be collected by tracking technologies
  - Webpages of Regulated Entities that address specific symptoms or health conditions, such as pregnancy or miscarriage
  - Webpages of Regulated Entities where users can search for a provider or schedule an appointment, even if the page does not require a log-in to perform the search

Tracking Technologies on Unauthenticated Pages

- OCR appears to distinguish
  - a general home page for a multi-specialty provider offering information about the provider's location and services (where tracking the IP addresses visiting the site would not constitute the collection and sharing of PHI) and
  - condition- or symptom-specific pages (where OCR indicates the tracking of IP addresses visiting the site would constitute the collection and sharing of PHI)
- OCR does not offer any guidance related to the homepages of single-specialty providers or providers that treat a single (or a handful of related) conditions
- OCR does not provide guidance on when a webpage's information is so specific to a symptom or health condition that information collected by a tracking technology on that page is PHI

The Bulletin's Clarifications and Reminders

- Describing the use of tracking technologies in a website's or mobile app's privacy policy, notice, or terms and conditions of use is insufficient for meeting HIPAA obligations
- Marketing uses of PHI collected through tracking technologies must be authorized in accordance with HIPAA (or fall within an exception) and website banners that ask users to accept or reject a website's use of tracking technologies, such as cookies, do not constitute a valid HIPAA authorization for marketing purposes
- De-identification of PHI by a tracking technology vendor prior to saving it does not change the vendor's status as a business associate
- Unless an exception applies, only the minimum amount of PHI necessary to achieve an intended purpose (which must be permitted under the Privacy Rule) may be disclosed to technology vendors
- When performing a HIPAA security risk assessment, the use of tracking technologies must be evaluated and the Regulated Entity should ensure that appropriate safeguards are in place to address security risks from tracking technologies
- The disclosure of PHI to tracking technology vendors without a BAA in place may constitute a breach under HIPAA and any such disclosure must be analyzed under the four-factor "low probability of harm" standard

State Privacy Law Considerations

State Laws – Health Information Privacy and Security

- Multiple approaches to protecting personally identifiable health information ranging from broader laws protecting personally identifiable consumer information to laws specific to sensitive types of identifiable information (e.g. mental health, substance use disorder, STD, genetic information, reproductive health)
- Washington's new "My Health, My Data" Act
  - Generally applies to entities that do business or target consumers in Washington and determine the purpose and means of collecting, processing, sharing, or selling of consumer health data
  - "Consumer health data" includes identifiable personal information that is linked or "reasonably linkable" to a consumer and that identifies the consumer's past, present, or future physical or mental health status and includes inferences from biometrics and location information
  - Requires detailed health data policies
  - Requires privacy notices and opt-in consent to collect data and for a broad range of uses and disclosures
  - Deletion requirements apply with virtually no exceptions
  - Prohibits geofencing around health care facilities to collect/use health data
  - Limited information level exemptions for research and data already regulated by other laws like HIPAA and 42 CFR Part 2
  - Private right of action under Washington's Consumer Protection Act

Slide 27

0

Probably also worth covering the CMIA and other HIPAA-esque state laws, especially since there is now some app-specific components of the law tha mirror the FTC's Health Breach Notification Rule in some regards.

Unknown, 1900-01-01T00:00:00Z

State Laws – Breach Notification

- 50 States; 50 Approaches
- All fifty states have breach notification laws related to the compromise of personally identifiable information, and no two states are exactly alike
  - Definition of PII varies and may include medical information
  - Timing of and method for notification varies
  - Exclusions and safe harbors vary (some states have an explicit safe harbor for encrypted information)
  - Some states have a private right of action while in others, enforcement is only carried out by the state Attorney General
- Essential for all health care companies to have a process in place to analyze breach reporting obligations

Key Takeaways

Key Takeaways

- Advertising and marketing activities can implicate multiple privacy laws
- Inferences that can be made about individuals by recipients need to be evaluated:
  - FTC believes an email or an IP address alone can disclose private information about consumers based on the entity sharing the data
  - OCR believes information collected prior to establishing a relationship with a consumer and inferences made by visiting web pages (even if unauthenticated) can be PHI
  - Websites and web pages that provide educational content regarding health conditions and treatments can create IHI according to FTC and OCR
- Obtain express authorization (in accordance with HIPAA if it applies) before collecting, using, and disclosing consumers' health information for marketing purposes
- Keep the company's privacy policy and other customer-facing statements current, factually accurate, and clear regarding marketing activities that result in the sharing of information with third parties
- De-identification of data by recipients does not address the issue of improper sharing

Key Takeaways

- Consider the risks of making public representations regarding HIPAA compliance and other privacy and security measures before making them and update any existing statements that are misleading or inaccurate
- Review current and prospective contracts with third parties to ensure applicable data sharing provisions align with applicable law (require a business associate agreement if necessary), information privacy and security policies and procedures, and public representations
- Ensure all staff are appropriately trained on policies, procedures, and practices with respect to the collection, use, and disclosure of user health information, and ensure that you are monitoring compliance with internal policies
- To the extent the use of tracking technologies may have resulted in unauthorized disclosure of health information to third parties, consult counsel for purposes of evaluating breach reporting obligations

What Does this Mean for the Life Sciences Industry?

Privacy in Life Sciences

Life sciences companies typically use and disclose significant amounts of health care data, and therefore should be auditing the collection, use and disclosure of IHI and updating privacy policies and other consumer-facing documents for accuracy

1 Understand how US privacy laws apply to your organization (and how they don't).

- *It's no longer just about whether HIPAA applies; you need to think about state laws, FTC Act, guidance, and enforcement.*
- *Don't forget about research-related requirements and exemptions.*
- *Compliance is starting to look more complex for companies that are not in scope of HIPAA.*

Privacy in Life Sciences

2 It's time to dust off those data maps / inventories.

- *According to the recent enforcement and guidance from FTC and OCR, life science companies may be using and disclosing more IHI than previously expected.*
- *Particularly re-visit the website specific processes and collection activities and press on the types of information captured by tracking technologies captured on these sites.*
- *Pay special attention to patient-directed websites – particularly when visiting such a page may indicate that the visitor may have a specific conduction.*
- *Don't forget websites that are integrated into products (such as portals), particularly because the review and update cycles for these sites are often tied to the product development lifecycle.*

Privacy in Life Sciences

3 Revisit training; consider additional role-based training.

- *Employees are frequently confused about what falls in and/or out of the scope of health information laws; these changes may require additional education.*
- *Highlight the unique challenge of websites – they never seem like the riskiest datasets for life science companies, but are public-facing and low-hanging fruit.*
- *For HIPAA covered entities, continue to press upon the "tough" identifiers*

Privacy in Life Sciences

4 Build / maintain that network of champions.

- *You only have two eyes, but a strong network of privacy champions can act as a first layer of defense and escalate issues in a way that e.g., the FTC called out in BetterHelp.*
- *Highlighting and building relationships with partners in digital communications and marketing functions will be increasingly important.*

MINTZ

5 Don’t talk the talk; just walk the walk.

- *What you put on your websites and notices are out there to be reviewed and scrutinized.*
- *Work with your digital communications and marketing teams to make sure that content on the site (and other public-facing materials) are accurate and kept up-to-date.*
- *Build these questions and considerations into a scalable privacy-by-design process to help ensure that these issues are flagged and tracked.*
- *Constant vigilance.*

Questions?

MINTZ

THANK YOU

Lara Compton
LDCompton@mintz.com // 424.259.4019

Kathryn F. Edgerton
KFEdgerton@mintz.com // 424.259.4030