COSMOS
Navigate the Compliance Universe

Compliance Today - March 2024

Lara Compton (ldcompton@mintz.com, linkedin.com/in/lara-compton/) is a Member of the Los Angeles office of Mintz, Levin, Cohn, Ferris, Glovsky and Popeo P.C.

Sophia Temis (stemis@mintz.com, linkedin.com/in/sophia-temis-80465b29b/) is an Associate in the New York Office of Mintz, Levin, Cohn, Ferris, Glovsky and Popeo P.C.

Madison Castle (mmcastle@mintz.com, linkedin.com/in/madison-castle-5a1a07114/) is an Associate in the Washington, DC office of Mintz, Levin, Cohn, Ferris, Glovsky and Popeo P.C.

HIPAA happenings: 2023 year in review

by Lara Compton, Sophia Temis, and Madison Castle

The U.S. Department of Health and Human Services Office for Civil Rights (OCR) had another busy year in 2023 in the wake of the COVID-19 pandemic and following the *Dobbs vs. Jackson Women's Health Organization (Dobbs)* decision. As will be subsequently discussed, federal agencies have moved to close the gaps in privacy protections for health information, with an eye toward protecting reproductive health information. Additionally, growing cybersecurity threats have increased the focus on preventing unauthorized access to health information.

Federal agency actions in the wake of the *Dobbs* decision

Tracking technologies

Heading into 2023, the healthcare industry saw a flurry of activity in response to the expansive position taken by OCR and the Federal Trade Commission (FTC) (collectively, the Agencies) regarding the applicability of the privacy laws that they enforce in response to the use of tracking technologies. This response appears to be part of a broader attempt by the Agencies to bridge health information privacy gaps, driven in part by concerns about inferences that can be made from information collected about consumers and the increasing amount of health-related information collected from consumers that is used for purposes other than healthcare (e.g., marketing, advertising, and other forms of monetization).

OCR guidance entering 2023

On December 1, 2022, OCR issued a bulletin highlighting the applicability of the HIPAA Privacy, Security, and Breach Notification rules to the use of online tracking technologies (Bulletin) by covered entities and business associates (collectively, Regulated Entities).[1] Notably, in the Bulletin, OCR interpreted the definition of protected health information (PHI) to capture information collected in the absence of a relationship between a Regulated Entity and an individual and information that is not specific to an individual's health. According to OCR, information collected from unauthenticated pages of a website can be PHI if the information on the page

might allow an inference about an individual's health, such as information collected from webpages pertaining to abortion or miscarriages.[2] In these circumstances, the information is health-related but is not necessarily specific to the individual researching the condition. The Bulletin does not have the force of law; however, it does indicate the agency's current thinking in terms of the information protected by HIPAA and entities that OCR could qualify as business associates (e.g., Facebook).

In an effort to combat OCR's broad interpretation of HIPAA applicability in the Bulletin, on November 2, 2023, the American Hospital Association, along with the Texas Hospital Association, Texas Health Resources, and United Regional Health Care System filed a lawsuit in Texas federal court arguing that, among other things, OCR violated various provisions of the Administrative Procedure Act (APA) in issuing guidance without going through the notice and comment proposed rulemaking process.[3] Many of the alleged APA violations arise from OCR's broad interpretation of what qualifies as PHI, which plaintiffs argue dramatically shifted healthcare providers' obligations under HIPAA without engaging in the required notice and comment rulemaking process.

FTC tracking technology enforcement

On February 1, 2023, the FTC announced its first enforcement action under the Health Breach Notification Rule[4] against GoodRx Holdings Inc. for its failure to notify consumers of its unauthorized disclosures of individually identifiable health information (IHI). The FTC also alleged GoodRx violated Section 5 of the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce"[5] by misrepresenting its privacy practices (including compliance with HIPAA) and using tracking pixels and other automated trackers in a manner that monetized and shared IHI with third-party advertisers without proper consumer notice or authorization.[6]

The FTC took similar enforcement actions against several other companies relating to the privacy of health information throughout 2023, including BetterHelp Inc.[7] and Easy Healthcare Corporation, the developer of the app Premom.[8] The FTC alleged that BetterHelp and Premom deceptively shared IHI for advertising and other purposes and failed to notify consumers of the unauthorized disclosure of their IHI.[9] In both cases, the FTC stated that consumers submitted IHI for purposes of receiving services, and these consumers were assured their information would remain protected by strict company privacy protocols.[10] According to the FTC, despite these assurances, both BetterHelp and Premom shared consumer IHI with third-party companies without their consent for advertising purposes. The enforcement actions resulted in Good Rx, BetterHelp, and Premom paying nearly $10 million, collectively, between civil monetary penalties and settlements to consumers.

OCR–FTC joint warning letter

On July 20, 2023, OCR and FTC sent a joint letter to approximately 130 hospital systems and telehealth providers warning them about "serious privacy and security risks related to the use of online tracking technologies."[11] The form of letter, shared publicly, stressed the importance of monitoring data flows of health information to third parties through tracking technologies and warned of enforcement against entities that fail to take corrective action to protect the privacy and security of individuals' health information.

FTC takeaways from recent enforcement actions

On July 25, 2023, the FTC published "key takeaways" from select health information privacy-related cases.[12] Among other things, in the takeaways, the FTC urged companies to:

- Understand what qualifies as health information (which, according to the FTC, includes anything that conveys information or enables inference about a consumer's health); and
- Be transparent, clear, and, if possible, specific with consumers about how they handle consumers' data protection and health information privacy.

Notably, the FTC also made it evident that companies should obtain express consumer consent before sharing sensitive health information and be clear and accurate about whether HIPAA applies, noting that touting HIPAA compliance, seals, or certifications may deceive consumers (especially since only OCR may determine whether an entity is in fact HIPAA compliant).

Overall tracking technology considerations

Considering the Agencies' guidance and enforcement, all entities that collect IHI (including PHI) should consider taking the following steps:

- Perform data mapping to understand the data collected from patients/consumers and identify the purposes for which it is used and shared, taking into account what health information could be inferred by the data collected, not just the data itself;
- Identify what privacy and security laws apply to the IHI collected and be clear about which laws apply in public-facing statements, keeping in mind that different privacy laws could apply to different lines of business;
    - Avoid making "HIPAA compliant" type claims and using misleading HIPAA seals and logos in public-facing documents;
    - Compare current use and sharing of IHI with statements made to the public regarding such use and sharing, and address any inaccuracies;
    - If IHI is shared with tracking technology vendors, confirm that all legally required authorizations and consents were obtained (e.g., consent or authorization for marketing) and necessary agreements are in place (for example, business associate agreements if PHI is involved); and
    - Contact counsel if it is determined that prior use and disclosure of IHI could have resulted in an unauthorized use or disclosure.

Proposed Privacy Rule: "Reproductive Health Care"

In April 2023, OCR proposed the "HIPAA Privacy Rule to Support Reproductive Health Care Privacy" (Proposed Rule), which aims to protect patient–provider confidentiality and prevent private medical records from being used against people for merely seeking, obtaining, providing, or facilitating lawful reproductive healthcare.[13] Among other things, the Proposed Rule would prohibit Regulated Entities from:

- "using or disclosing PHI where the PHI would be used for a criminal, civil, or administrative investigation into or proceeding against any person in connection with seeking, obtaining, providing, or facilitating lawful reproductive health care, or
- "identifying any person for the purpose of initiating such an investigation or proceeding . . ." (referred to as "prohibited purposes").

This new prohibition would apply when the investigation or proceeding relates to care that is provided outside of the state where the investigation or proceeding is authorized and is lawful in the state where the care was provided. Additionally, OCR proposed that third-party reproductive health information requests be accompanied by an attestation stating that the information will not be used for prohibited purposes. The Proposed Rule would not create a blanket prohibition on disclosure of reproductive health PHI. Instead, it focuses on the purpose of the disclosure or the use of such reproductive health PHI, as opposed to the type of PHI requested or the type of Regulated Entity that receives the request. OCR notes that the Proposed Rule is constructed this way to prevent slowing or limiting providers from coordinating care.

The Proposed Rule, if finalized, would create a new category of PHI subject to special protections; therefore, Regulated Entities should begin considering what additional policies, procedures, and safeguards might be necessary for compliance, keeping in mind that, if finalized, the rule would apply to information that is clearly considered reproductive health information and (according to the Bulletin) inferences that relate to reproductive health.