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.

OCR enforcement actions related to cyberattacks, patients' right to access, and business associate relationships

Each year, OCR makes HIPAA enforcement case examples available on its website.[14] The following is a summary of the resolution agreements posted to the OCR website as of December 15, 2023.

Covered entity enforcement

OCR entered into four resolution agreements with covered entities arising from OCR's investigations of impermissible disclosures and cybersecurity incidents identifying potential HIPAA violations, including, among others, alleged failure to:

- "Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information;"[15]
- "Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements" of the Security Rule;[16]
- Implement sufficient system access review procedures;[17] and
- Implement authentication procedures.[18]

Civil monetary penalties assessed to each of the four covered entities ranged from $30,000 to $1.3 million, and each resolution agreement was accompanied by a corrective action plan with a term of two to three years, which usually included requirements to update cybersecurity policies and procedures and train workforce to identify and prevent such future breaches.[19]

Business associate enforcement

OCR entered into three resolution agreements with business associates following breaches caused by cyberattacks and unauthorized server infiltrations. These resolution agreements were based on potential HIPAA violations, including, but not limited to, the business associates' failure to:

- "Implement procedures to regularly review records of information system activity, such as audit logs,

access reports, and security incident tracking reports";[20]

- "Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information";[21]
- Assess potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI (ePHI) held by its business associate was not sufficiently accurate or thorough; [22] and
- Enter into business associate agreements with subcontractors.[23]

Two of the breaches resulted from insecure servers, while one was the product of cybercriminal ransomware known as GandCrab.[24] Nearly 450,000 individual records were collectively exposed through these breaches, and civil monetary penalties assessed to each of the three business associates ranged from $75,000 to $350,000. The resolution agreements were accompanied by corrective action plans with terms of two to three years involving development of a risk management plan, security policies and procedures, among other obligations.

Patients' right to access

In 2023, three covered entities entered into resolution agreements with OCR for allegedly failing to provide patients and their representatives with timely access to their "designated record set" as required under HIPAA's Privacy Rule ("Right of Access").[25] The number of publicized Right of Access resolution agreements decreased in 2023 as compared to years 2021 and 2022, which each had around 12 publicized enforcements per year.[26] Of the three 2023 enforcement actions, two could involve additional state law requirements and limitations on access to patient records by their representatives:

1. A licensed psychotherapy counselor refused to provide a parent with access to the records of his minor child, which OCR settled for $15,000.[27]
2. A lab failed to provide timely access to medical records of a decedent, which OCR settled for $16,500.[28]

It is unclear whether state law played a role in these two instances, but it appears each covered entity's documentation was not adequate to support record access denials.

Overall takeaways from recent OCR actions

In light of OCR's 2023 enforcement activity, Regulated Entities should focus on preventing threats to health information privacy and security and consider taking the following steps:

- Provide more frequent reminders to staff regarding common mistakes that lead to impermissible disclosures and cybersecurity incidents;
- Conduct regular phishing and ransomware attack simulations;
- Increase the frequency of security assessments, vulnerability testing, systems activity review, and systems access audits;
- Use all reasonably available tools to prevent and monitor for unauthorized access to information systems; and
- Review medical records access policies and state laws to confirm whether more stringent limitations must

be addressed in patient/representative access denial communications, policies and procedures, and related documentation.

HIPAA security tools and best practices

Under HIPAA, Regulated Entities must institute certain authentication procedures to protect the privacy and security of patient health information; however, the Security Rule does not require implementation of specific authentication solutions. Though, in June 2023, OCR released a HIPAA Cybersecurity Authentication newsletter, making it clear that phishing-resistant, multi-factor authentication (MFA) is a best practice that should be implemented where appropriate.[29] The newsletter describes multiple cyberattacks that resulted from use of weak passwords and exploitation of old administrator accounts—which could have been prevented by stronger authentication processes—and provides guidance on how to "lock your cyber door," as subsequently discussed.

Best user authentication practices to thwart cyberattacks

The newsletter recommends that authentication processes include the use of three distinct factors to corroborate the identity of the person attempting to access an account:

1. Something you know – like passwords and identification numbers;
2. Something you have – security tokens or smart identification cards; and
3. Something you are – like fingerprints and facial recognition.

These factors may be used independently (single-factor authentication) or in tandem with one another (MFA). Experts generally advocate for using MFA, as it enhances security in instances when one of the three factors is compromised and can impede an attacker's efforts to gain unlawful access to a Regulated Entity's ePHI.

HIPAA Security Rule — Authentication and risk assessments

The newsletter points out that different touchpoints may present different levels of risk. Therefore, Regulated Entities must consider all access points to information systems when conducting security risk assessments, and they will need to employ policies and procedures based on particular vulnerabilities. For example, remote access to ePHI presents specific vulnerabilities that are nonexistent when accessing records in person. OCR also notes an increased risk associated with using:

- Privileged accounts that can override and grant additional controls to attackers; and
- Tools such as" virtual machine managers or storage area network tools" that support the entire technology infrastructure of Regulated Entities.

Notably, OCR and the Office of the National Coordinator for Health Information Technology released version 3.4 of its HIPAA Security Risk Assessment Tool a few months after the newsletter was released—an updated and more user-friendly version of its predecessor.[30]

Telehealth and HIPAA

During the COVID-19 pandemic, OCR waived certain HIPAA requirements to rapidly implement remote communication technologies during the COVID-19 public health emergency (PHE). These waivers ended on August 9, 2023, after a 90-day transition period.[31]

Following the expiration of the transition period, OCR released two resource documents in October 2023 regarding the privacy and security risks posed by telehealth services.[32] The documents are meant to separately inform patients and providers of the risks involved with the use of telehealth technology and best practices for mitigating such risks in the post-PHE era. Among other things, OCR encourages (but does not require) providers to:

- Warn patients about the potential risks of telehealth, including computer viruses, unauthorized access, and accidental disclosures, and how to protect their privacy in light of these threats;
- Educate patients about the steps they can take to protect themselves, for example, taking telehealth appointments in a private location and updating software installed on their devices, which often improves software vulnerabilities exploited by cybercriminals; and
- Communicate when and how patients will be contacted for appointments to decrease the likelihood that patients fall victim to phishing attempts and illegitimate links via email or text message.

OCR also reminded providers that in using telehealth, they need to take appropriate steps to ensure that communications with an individual with a disability or language barrier are as effective as communications with others by providing auxiliary aids and providing written translated information or a qualified interpreter in order to comply with applicable disability and nondiscrimination laws.[33]

2023 in review

In looking back at 2023, key compliance considerations include:

- Entities collecting consumer information—including those not subject to HIPAA—should review use of tracking technologies for IHI collection and determine whether the required consents and authorizations were obtained and necessary agreements between companies exchanging or transferring consumer information is in place.
- Entities with access to identifiable consumer information should regularly conduct data mapping and security risk assessments to identify (and then mitigate) privacy and security risks, keeping in mind FTC's and OCR's broad interpretation of what qualifies as IHI and PHI and potential upcoming changes applicable to reproductive health information.
- Regulated Entities should implement MFA if feasible to prevent unauthorized access to PHI.
- Regulated Entities should regularly educate employees and patients regarding mitigating privacy and security risks.
- All entities collecting IHI should provide clear and accurate information to patients and consumers about IHI that is collected through such entities' websites and applications, what laws apply to the IHI, and how the IHI may be used and disclosed. If HIPAA applies to only certain activities or business lines, this information should be provided.
- All entities collecting IHI should review websites and remove misleading statements and seals claiming HIPAA compliance.

Takeaways

- Health information privacy is a priority for federal agencies, even when HIPAA doesn't apply.

- According to the U.S. Department of Health and Human Services Office for Civil Rights, protectged health information (PHI) not only includes identifiable health information but also identifiable health inferences.
- Collection of information using tracking technologies on websites and applications should be carefully reviewed for HIPAA compliance and other privacy risks.
- Security best practices, such as multi-factor authentication, should be implemented by regulated entities whenever possible.
- If finalized, the "HIPAA Privacy Rule to Support Reproductive Health Care Privacy" will create a new category of PHI subject to special protections.

1 U.S. Department of Health and Human Services, Office for Civil Rights, "HHS Issues Bulletin on Requirements under HIPAA for Online Tracking Technologies to Protect the Privacy and Security of Health Information," news release, December 1, 2022), https://www.hhs.gov/about/news/2022/12/01/hhs-office-for-civil-rights-issues-bulletin-on-requirements-under-hipaa-for-online-tracking-technologies.html.
2 U.S. Department of Health and Human Services, Office for Civil Rights, "HHS Issues Bulletin on Requirements under HIPAA for Online Tracking Technologies to Protect the Privacy and Security of Health Information."
3 American Hospital Association et al. v. Melanie Fontes Rainer et al. No. 4:23-cv-01110-P (N.D. Texas. 2023).
416 C.F.R. § 318.
5 "Federal Trade Commission Act—Section 5: Unfair or Deceptive Acts or Practices," *Consumer Compliance Handbook*, June 2008, https://www.federalreserve.gov/boarddocs/supmanual/cch/200806/ftca.pdf.
6 Federal Trade Commission, "FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising," news release, February 1, 2023, https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising.
7 Federal Trade Commission, "FTC to Ban BetterHelp from Revealing Consumers' Data, Including Sensitive Health Information, to Facebook and Others for Targeted Advertising," news release, March 2, 2023, https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-ban-betterhelp-revealing-consumers-data-including-sensitive-mental-health-information-facebook.
8 Federal Trade Commission, "Ovulation Tracking App Premom Will be Barred from Sharing Health Data for Advertising Under Proposed FTC Order," news release, March 17, 2023, 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.
9 Lesley Fair, "FTC–HHS joint letter gets to the heart of the risks tracking technologies pose to personal health information," Federal Trade Commission, Business (blog), July 20, 2023, https://www.ftc.gov/business-guidance/blog/2023/07/ftc-hhs-joint-letter-gets-heart-risks-tracking-technologies-pose-personal-health-information.
10 Federal Trade Commission, "FTC to Ban BetterHelp from Revealing Consumers' Data, Including Sensitive Health Information, to Facebook and Others for Targeted Advertising" ; Federal Trade Commission, "Ovulation Tracking App Premom Will be Barred from Sharing Health Data for Advertising Under Proposed FTC Order."
11 U.S. Department of Health and Human Services, Office for Civil Rights, "Use of Online Tracking Technologies," template letter, July 20, 2023, https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf.
12 Elisa Jilson, "Protecting the privacy of health information: A baker's dozen takeaways from FTC cases," Federal Trade Commission, Business (blog), July 25, 2023, https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases.
13 HIPAA Privacy Rule To Support Reproductive Health Care Privacy, 88 Fed. Reg. 23,506 (proposed April 17, 2023) (to be codified at 45 C.F.R. § 160, § 164), https://www.federalregister.gov/documents/2023/04/17/2023-

07517/hipaa-privacy-rule-to-support-reproductive-health-care-privacy.
14 U.S. Department of Health and Human Services, Office for Civil Rights, "Resolution Agreements," content last reviewed December 14, 2023, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html.
1545 C.F.R. § 164.308(a)(1)(ii)(A).
1645 C.F.R. § 164.316(a).
1745 C.F.R. § 164.308(a)(1)(ii)(B).
1845 C.F.R. § 164.312(c)(2).
19 U.S. Department of Health and Human Services, Office for Civil Rights, "Resolution Agreements."
2045 C.F.R. § 164.308(a)(1)(ii)(D).
2145 C.F.R. § 164.308(a)(1)(ii)(A).
2245 C.F.R. § 164.308(a)(1)(ii)(A).
2345 C.F.R. § 164.504(e)(5).
24 U.S. Department of Health and Human Services, Office for Civil Rights, "Doctors' Management Services, Inc. Resolution Agreement and Corrective Action Plan," news release, October 31, 2023, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/dms-ra-cap/index.html.
2545 CFR §164.524.
26 U.S. Department of Health and Human Services, Office for Civil Rights, "Resolution Agreements."
27 U.S. Department of Health and Human Services, Office for Civil Rights, "David Mente, MA, LPC Resolution Agreement and Corrective Action Plan," content last reviewed May 8, 2023, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/mente-ra-cap/index.html.
28 U.S. Department of Health and Human Services, Office for Civil Rights, "Life Hopes Resolution Agreement and Correction Action Plan," content last reviewed January 14, 2023, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/life-hopes-ra-cap/index.html.
29 U.S. Department of Health and Human Services, Office for Civil Rights, "June 2023 OCR Cybersecurity Newsletter," content last reviewed June 29, 2023, https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-june-2023/index.html.
30 Office of the National Coordinator for Health Information Technology, "Security Risk Assessment Tool," accessed January 18, 2024, https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool.
31 U.S. Department of Health and Human Services, Office for Civil Rights, "HHS Office of Civil Rights Announces the Expiration of COVID-19 Public Health Emergency HIPAA Notifications of Enforcement Discretion," news release, April 11, 2023, https://www.hhs.gov/about/news/2023/04/11/hhs-office-for-civil-rights-announces-expiration-covid-19-public-health-emergency-hipaa-notifications-enforcement-discretion.html.
32 U.S. Department of Health and Human Services, Office for Civil Rights, "HIPAA and Telehealth," content last reviewed October 18, 2023, https://www.hhs.gov/hipaa/for-professionals/special-topics/telehealth/index.html.
33 U.S. Department of Health and Human Services, Office of Civil Rights, "Resource for Health Care Providers on Educating Patients about Privacy and Security Risks to Protected Health Information when Using Remote Communication Technologies for Telehealth," content last viewed October 17, 2023, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/resource-health-care-providers-educating-patients/index.html.