HIPAA Changes 2023:
A Return to Normalcy?

In November of 1918, the First World War (naively called "The Great War") ended. (For people who appreciate or read into symmetry, World War I ended at the 11th hour on the 11th day of the 11th month of 1918). The League of Nations, the peacekeeping body and the precursor to today's United Nations, was founded in January 1920 by President Woodrow Wilson and held its first meeting in November of that year.

Another important event took place that November—the Presidential election. Republican presidential candidate Warren Harding, sensing Americans were tired of war, and tired of fighting for peace (ironically, although Wilson formed the League of Nations, the U.S. refused to join), campaigned on the slogan, "A return to normalcy." His incorrect word usage (the word "normalcy" did not exist when he used it) may have been unserious, but the election results meant business: Harding won in a rout. Normalcy seemed to be back on the menu.

From 2020 to 2022, the U.S. government was engaged in a war of its own, fighting COVID-19 (or trying to, anyways, depending on who you ask). The Department of Health and Human Services (HHS), the federal agency designed to enhance the well-being of Americans, spent much time and resources navigating this public health crisis.

While COVID-19 has not formally ended, many Americans are anxious to put the events of the last two years behind them—to return to normalcy. As we got further into 2022, HHS's Office for Civil Rights (OCR) became less focused on COVID-19 public health initiatives and more focused on traditional areas of concern. Enforcement of the Privacy Rule's right of access provision, and ensuring patient PHI is not impermissibly used or disclosed, took center stage in 2022 and are poised to receive additional emphasis in 2023. The details of HIPAA changes

2023 are described below.

HIPAA Changes 2023: Return to Access

OCR completed investigation of 17 patient right of access cases in 2022. Fifteen of these resulted in a Resolution Agreement (Settlement), and two resulted in the imposing of a civil monetary penalty. The first 2022 resolution agreements were announced in March of 2022. The most recent resolution agreement (at time of writing) was announced on December 15, 2022.

OCR launched its Right of Access Initiative in 2019, bravely taking the radical stand that the rules requiring covered entities to act on patient medical requests must be enforced. In 2019, there were two right of access settlements/fines. In 2020, there were 11. In 2021, there were 12. In 2022, there were 17. Forty-two (42) in total.

In 2022, OCR emphasized specific aspects of right of access non-compliance, which are recounted below. Providers may expect that these areas of non-compliance will be on OCR's radar in 2023.

Don't Look a Gift Horse in the Mouth: Act on Technical Assistance

ACPM Podiatry Group is an Illinois practice. In early April 2019, OCR received an initial complaint from Richard Lindsey ("Complainant"), a former patient who alleged that ACPM refused to provide him with his requested medical records. On April 18, 2019, OCR provided ACPM with written technical assistance regarding the Privacy Rule's right of access standard (basically, OCR explained what the standard means) and then closed the matter.

OCR then received a second complaint from Mr. Lindsey, alleging that ACPM still needed to provide the medical records after he made numerous requests. ACPM did not respond to multiple data requests from OCR, nor to OCR's Letter of Opportunity and Notice of Proposed Determination (this is legalese for saying that ACPM blew off OCR's investigation). Having given ACPM ample time to cooperate with the investigation, OCR issued a Notice of Final Determination and imposed a civil money penalty of $100,000.

In July of 2020, a few months before OCR issued the November 2020 Letter of Opportunity (a Letter of Opportunity is a document alerting a provider that there are preliminary indications of non-compliance; the letter also allows the provider to submit written evidence of mitigating factors or affirmative defenses for OCR's consideration in making a determination of the amount of a civil monetary penalty).

ACPM finally got off its back, rousing itself to provide Mr. Lindsey with copies of his records. However, Mr. Lindsey informed OCR that the records he received—618 days after he made the initial records request—were incomplete. APCM provided no explanation as to why it could not provide all of the records.

Lesson: *OCR provides technical assistance as a way of informally resolving complaints without having to impose more serious measures. When advice is offered, it's a good idea to follow it.*

Records Cannot be Held Hostage

On March 27, 2020, HHS received a complaint against Danbury Psychiatric Consultants (DPC), alleging that DPC failed to provide access to the complainant's protected health information (PHI).

HHS's investigation revealed that, on March 24, 2020, the complainant made an access request for her PHI. DPC failed to respond timely to the complainant's access request. DPC also withheld complainant's access on the basis that the complainant had an outstanding balance, and required a signed request or authorization request (a provider may require that a request be in writing, but, if it imposes this requirement, it must notify its patients beforehand of the requirement).

DPC failed to provide access to all the complainant's PHI until September 14, 2020, after OCR initiated its investigation.

This conduct—holding records hostage for payment—is prohibited under the right of access provision. For its trouble, DPC settled with HHS by agreeing to pay HHS $3,500 and submit to a two-year corrective plan. Under the CAP, DPC must develop policies and procedures on the HIPAA right of access provision, and must train employees on these policies and procedures.

Lesson: *Patient records are not bargaining chips.*

Clear Up Misunderstandings

Fallbrook Family Health Center, a Nebraska clinic, failed to provide a patient with a complete copy of her designated record set even though she requested it in writing three separate times.

FFHC claimed it failed to provide access due to a former workforce member's misunderstanding of an individual's access rights under HIPAA. The nature of the misunderstanding is not publicly known. As a result of OCR's investigation, FFHC sent complainant a copy of her complete designated record set on June 19, 2020. Fallbrook agreed to take corrective actions and paid $30,000 to settle a potential violation of the right of access standard.

The corrective action plan requires FFHC to "review, and to the extent necessary, revise its policies and procedures related to the right of access to protected health information (PHI)," and to train staff (including new staff, within 30 days of hire) on these policies and procedures. Having effective written policies and procedures, and training employees on these, should prevent further misunderstandings on the meaning of the phrase "provide access" from happening.

I've Got the Power

On July 20, 2020, HHS received a complaint against MelroseWakefield from an individual ("Complainant") alleging that she requested the protected health information (PHI) of her mother from MelroseWakefield and had been denied access to the requested records.

HHS's investigation revealed that, on June 12, 2020, the complainant made a valid access request for her mother's PHI, having attached documentation—a durable power of attorney—verifying that she was her mother's personal representative. A durable power of attorney with the right to make healthcare decisions must be honored. In this case, the complainant was not provided access to the records because of MelroseWakefield's mistaken belief that the durable power of attorney did not allow the complainant to secure the records.

After the complainant notified OCR of the denial of access, OCR notified MelroseWakefield of the allegations. MelroseWakefield's collection of minds then (so the record states) reviewed the power of attorney documentation anew, and determined that the complainant should have received access to the records based on her initial request.

The complainant was provided access on October 20, 2020. OCR subsequently settled the matter with MelroseWakefield for $55,000. MelroseWakefield also agreed to the imposition of a one-year corrective action plan.

Under the CAP, the practice must develop policies and procedures that explain to workforce members how to verify the identity and authority of a personal representative for the purposes of a request for access to PHI. These policies and procedures must spell out what documentation, if any, an individual must provide to prove their identity and authority.

Bills, Bills, Bills

On August 31, 2020, OCR received a patient complaint alleging that provider Memorial Hermann Health System failed to provide the patient with her complete medical and billing records. Complainant alleged that she had made five separate requests for these records between June 2019 and January 2020, and that Memorial failed to take timely and compliant action upon the requests.

OCR initiated a formal investigation, in which it determined that Complainant asked for an itemized billing statement on July 3, 2019; that Memorial received the request; and that Memorial did not comply in full until March 26, 2022—564 days after the initial request.

Lesson: *Medical records include billing records.*

Let's Be Reasonable

In two 2022 right of access cases, OCR called the provider out for charging patients excessive fees for copies of their records. The right of access prohibits excessive fees.

In its March 2022 Resolution Agreement with provider Jacob & Associates, OCR noted that this provider failed to provide timely access to PHI to a patient who requested that access. OCR also stated that the provider charged an unreasonable fee that was not cost-based, as required by law (incidentally, the provider had also required Complainant to travel to its office to complete its form to exercise her right to access, imposed a flat fee of $25 per medical records request, initially provided an incomplete (one page) paper copy of the records, failed to designate a Privacy Officer, and failed to include required content in its Notice of Privacy Practices).

In September of 2022, OCR entered into a Resolution Agreement with Great Expressions Dental Centers of Georgia, P.C. (GEDC-GA). The Complainant alleged that GEDC-GA failed to provide her with access to her medical records; in response to her November 25, 2019 access request, GEDC-GA had required that the Complainant pay a $170 copying fee before GEDC-GA would provide the Complainant with the requested medical records.

GEDC-GA did not contact the Complainant to send her the requested medical records until February 2, 2021. OCR concluded that GEDC-GA failed to provide timely access, and that GEDC-GA imposed an unreasonable fee not based on the costs of reproduction. OCR settled the matter with GEDC-GA for $80,000.

Note: *Providers should know for 2023 (and should train their staff to know) that patients, when requesting their own records for their own use, may only be charged a "reasonable, cost-based fee," per the right of access provision of the Privacy Rule. Also, providers should know that if a state law allows the provider to charge a higher fee than HIPAA allows and that the state law fee is "per page," not tied to the actual cost of copying the records, the provider must charge the lower, HIPAA fee.*

HIPAA Changes 2023: Return to Authorization

On June 24, 2022, the Supreme Court of the United States handed down its opinion in Dobbs v. Jackson Women's Health Organization. The question the Court was asked to decide in Dobbs was, "Are all pre-viability abortions always unconstitutional?" To this question, the Court answered "no."

To get to "no," the Court evaluated two of its prior precedents. The first of this was Roe v. Wade, decided in 1973. In Roe, the Court held that a woman has a constitutionally protected liberty interest in terminating a pregnancy up to the point of viability.

19 years later, the Court largely affirmed this ruling, in Planned Parenthood of Southeastern Pennsylvania v. Casey (Casey). In Casey, the Court held that a state could not place an "undue burden" on the right to terminate a pre-viability pregnancy.

To get to "no" in Dobbs, the Court felt bound to decide whether Roe and Casey were still good law. The Court found that they were not, and overruled both decisions.

In its opinion, the Court noted that it was not "outlawing abortion." Rather, the Court noted that, by removing the status of the right to terminate a pregnancy as constitutionally protected, it was returning the issue to each state. As a result, each state may now pass its own laws on whether, and up to what point in a pregnancy, to permit abortion.

How HIPAA Fits into the Picture

HIPAA limits covered entities' and business associates' ability to use or disclose protected health information. In the wake of Dobbs, HHS has issued guidance that addresses how federal law and regulations protect individuals' protected health information (PHI) relating to abortion and other sexual and reproductive healthcare. HIPAA changes 2023 may include additional guidance.

Just look at the thoroughness of the Post-Dobbs guidance HHS has already issued in 2022.

Post-Dobbs Guidance on Disclosure of PHI

HHS guidance issued in the wake of Dobbs describes the Privacy Rule's use and disclosure restrictions. "The Privacy Rule permissions for disclosing PHI without an individual's authorization for purposes not related to healthcare, such as disclosures to law enforcement officials, are narrowly tailored to protect the individual's privacy and support their access to health services." This guidance provides examples of when covered entities may disclose PHI without written individual authorization.

Disclosures Required by Law

The Privacy Rule permits but does not require covered entities to disclose PHI about an individual, without the individual's authorization, when such disclosure is required by another law and the disclosure complies with the requirements of the other law.

"Required by law" means that there is a law that contains a mandate that compels an entity to use or disclose the PHI, and that mandate can be enforced in a court of law. When a disclosure is "required by law," the covered entity or business associate may only disclose that which the law requires disclosure of. A disclosure of PHI that exceeds what the law demands is not a permissible disclosure.

HHS guidance provides an example of a permissible disclosure: An individual goes to a hospital emergency department while experiencing complications related to a miscarriage during the tenth week of pregnancy. A hospital workforce member suspects the individual of having taken medication to end their pregnancy. The relevant state or other law prohibits abortion after six weeks of pregnancy but does not require the hospital to report individuals to law enforcement.

Since the state law does not require the reporting, the Privacy Rule does not permit such disclosure under the "required by law" provision discussed above. If a provider were to disclose the information, the disclosure would be impermissible, and constitute a breach of unsecured PHI. Where state law does not expressly require such reporting, the Privacy Rule would

not permit a disclosure to law enforcement under the "required by law" permission. Therefore, such a disclosure would be impermissible and constitute a breach of unsecured PHI, requiring notification to HHS and the individual affected.

Disclosures for Law Enforcement Purposes

The Privacy Rule permits but does not require covered entities to disclose PHI about an individual for law enforcement purposes "pursuant to process and as otherwise required by law," under certain conditions.

A law enforcement request made "pursuant to process" means a request made through such legitimate processes as a court order or court-ordered warrant, or a subpoena or summons. A provider may, if a law requires disclosure, disclose PHI to a law enforcement request made pursuant to process, by disclosing only the requested PHI, and no more.

HHS provides two examples of the "law enforcement purposes" component of the Privacy Rule:

- **Example 1:** A law enforcement official goes to a reproductive healthcare clinic and requests records of abortions performed at the clinic. Under the HIPAA regulations, if the request is not accompanied by a court order or other mandate enforceable in a court of law, the Privacy Rule would not permit the clinic to disclose PHI in response to the request. Therefore, such a disclosure would be impermissible and constitute a breach of unsecured PHI requiring notification to HHS and the individual affected.
- **Example 2:** A law enforcement official presents a reproductive healthcare clinic with a court order requiring the clinic to produce PHI about an individual who has obtained an abortion. Because a court order is enforceable in a court of law, the Privacy Rule would permit but not require the clinic to disclose the requested PHI. The clinic may disclose only the PHI expressly authorized by the court order.

Expect HIPAA updates in 2023 to consist of additional guidance on when providers and PHI they hold may and may not be used in the service of state abortion investigations.

HIPAA Changes 2023: Return to Appropriate Use of Technology

Healthcare providers frequently use online tracking technologies—scripts or codes on a website or mobile app used to gather information about users as the users interact with the site or app. These technologies frequently have access to PHI. HHS recently issued a guidance bulletin to raise awareness of the inappropriate use of online tracking technologies.

The bulletin discusses how the HIPAA rules apply to different types of online tracking technology, including tracking on user-authenticated webpages, unauthenticated webpages, and within mobile apps.

User-Authenticated Pages

User-authenticated webpages, such as patient or health plan beneficiary portals, require a user to first log in with their credentials. A provider's user-authenticated webpage generally has access to PHI. To protect user privacy, HIPAA-covered entities must configure user-authenticated webpages that include tracking technologies to allow those technologies to only use and disclose PHI as permitted by the Privacy Rule. HIPAA-covered entities must ensure that any ePHI collected by such technologies is protected and secured in compliance with the Security Rule.

In addition, when an online tracking technology performs business associate functions for a HIPAA regulated entity, the regulated entity must ensure that any disclosures made to the technology vendor are permitted by the Privacy Rule.

Online Tracking Technology on Unauthenticated Webpages

A provider may maintain an unauthenticated webpage. An unauthenticated webpage does not require patient login as a precondition to access. Webpages with general information, such as provider's location or services, may be unauthenticated. Online tracking technologies on an unauthenticated webpage generally do not have access to PHI. If an individual must enter credentials or registration information on the login page to access the portal, the information collected by the tracking technology is considered to be PHI, protected by HIPAA.

Tracking technologies on a provider's unauthenticated webpage that allow individuals to search for doctors or schedule appointments without entering credentials may also have access to PHI. If these technologies collect individuals' email addresses and/or IP addresses when the individual makes the search, the provider is, in effect, disclosing PHI to the online tracking technology vendor. The result? HIPAA applies, again.

Online Tracking Technology within Mobile Apps: Who's the Collector?

Providers may offer mobile apps to individuals. These apps allow individuals to help manage their health information or to pay bills electronically. The apps collect information typed by the user or uploaded into the app. The apps may also collect information provided by the app user's device, such as fingerprints, network location, or device ID—a movable feast of PHI. When such PHI is collected, the provider must ensure that whatever PHI the app uses or discloses is in accordance with HIPAA.

Does HIPAA Ever Not Apply?

A different result presents when the user voluntarily downloads or enters data into a mobile device that was not developed or offered by or on behalf of the provider. Here, HIPAA does not apply. The provider is not creating, transmitting, maintaining, or receiving PHI. The provider is not out of a legal thicket, however. Other regulations, such as the FTC's Health Breach Notification rule, may apply. This rule regulates impermissible disclosures made by mobile health apps.

Online Tracking Technology: HIPAA Compliance Obligations

Providers in 2023 should be mindful of avoiding PHI pitfalls when using online tracking technologies. Providers must ensure that all disclosures of PHI to an online tracking technology are permitted by the Privacy Rule, and, unless an exception applies, must also ensure that only the minimum necessary PHI to achieve the intended disclosure purpose is disclosed.

Also, providers should address the use of tracking technologies in their risk analyses and risk remediation processes. Providers should also implement appropriate administrative, physical, and technical safeguards, (such as encryption, access controls, authentication controls, and audit controls), when they access ePHI stored in the tracking technology vendor's infrastructure. These controls ensure that ePHI is protected from unauthorized access.

Don't be surprised if 2023 HIPAA changes include issuance of further guidance on online tracking technologies, along with greater enforcement to ensure that providers who use online tracking technologies, use them only as allowed by HIPAA.

HIPAA Changes 2023: Remember This One?

HHS has one additional weapon in its 2023 stockpile to strengthen Privacy Rule protections: its Notice of Proposed Rulemaking to modify the HIPAA privacy rule. If HHS pulls the trigger and makes the proposed rule final, HIPAA 2023 Privacy Rule Changes may be significant—for enhancing patients' rights to access their health information, and for adding obligations on providers to ensure that they provide this access. Patient and privacy advocates have been pushing for this enhanced protection—this normalcy—for a decade, given the last major changes to the HIPAA Privacy Rule were made in 2013.

Daniel Lebovic, ESQ, Corporate Counsel and Technical Content Manager, Compliancy Group. Mr. Lebovic has 15+ years of regulatory compliance and contract management experience. His background makes him uniquely able to translate HIPAA regulations into content that those without legal knowledge can easily understand.

Need assistance with HIPAA compliance? Compliancy Group gives healthcare professionals confidence in their compliance plan, increasing client loyalty, and profitability of their business while reducing risk. Find out more about Compliancy Group and HIPAA compliance. Get compliant today! https://compliancy-group.com