

☆ Helping the public understand uses and disclosures of PHI

February 4, 2019 | Briefings on HIPAA

In recent months, OCR [announced](#) its plans to launch an education program on patients' rights in response to the national opioid crisis. In their [request for information](#) (RFI), which closes for comment on February 12, OCR has expressed concern that providers and other covered entities (CEs) may be reluctant to inform and involve the loved ones of individuals facing health crises like opioid use disorder or serious mental illness (SMI) for fear of violating HIPAA.

The HIPAA Privacy Rule aims to give patients control over how their information is used, while still allowing for the flow of health information needed to provide and promote quality care and to protect the public's health and well-being. Situations involving patients with sensitive conditions like opioid use disorder and SMI can be difficult to navigate for everyone involved.

So what are the most important things patients need to know about their privacy rights, especially patients with sensitive conditions like opioid use disorder or SMI? While OCR's education program is still in development, covered entities (CE) can help keep patients and their families informed of their privacy rights under HIPAA. Here, we look at some common misconceptions about privacy under HIPAA and point to the information that all patients need to know.

Consent and authorization

It's important that patients understand the difference between "consent" and an "authorization." Obtaining consent, which HHS defines as written permission from individuals to use and disclose their protected health information (PHI) for treatment, payment, and health care operations (TPO) is optional under the Privacy Rule for all CEs (see 45 *CFR* § 164.506(b)). By contrast, authorization gives CEs permission to use specified PHI for specified purposes, which are generally purposes other than TPO or to disclose PHI to a third party specified by the individual (see 45 *CFR* § 164.508). Some situations that require authorization include disclosures to a life insurer for coverage purposes or disclosures to an employer of the results of a pre-employment physical or lab test.

In practice, an authorization is a more customized document that will be detailed and limited in scope, explains **Rita Bowen, MA, RHIA, CHPS, CHPC, SSGB**, vice president of privacy, compliance, and HIM policy at MRO in Norristown, Pennsylvania. Most facilities have an exclusive authorization. When a patient comes in, they are given an authorization form and can check off specific types of sensitive information like HIV status, opioid use disorder, or STDs that they may not wish to have released, and give authorization for release of that

information, which would carry over to things like court appearances and subpoenas. An inclusive authorization form leaves it up to the patient to inform the provider what not to include. In other words, the patient must state whether or not they object to the release of sensitive information, Bowen adds.

It's important to note that sensitive information like substance use disorder which would also fall under 42 *CFR* Part 2 legislation (which is under the authority of the Substance Abuse and Mental Health Services Administration) applies to facilities that receive federal funds. A patient in the emergency room at a non-Part 2 facility falls under HIPAA but not Part 2 restrictions. Some individuals may be under the impression that sensitive information is redacted, Bowen says. Although providers can separate information that needs to be shared from the rest of the medical record, this can be difficult to accomplish in some EHRs.

Determining decision-making capacity

Obtaining consent is optional under HIPAA because consent refers to routine healthcare operations like treatment, which the patient is usually voluntarily seeking. However, in cases where the patient is incapacitated or unconscious, or if there is a serious and imminent threat to a patient's health or safety, then physicians can determine whether patients have decision-making capacity to consent to their information being disclosed.

If the provider determines the patient does not have decision-making capacity, HIPAA allows physicians to disclose information without consent when it is in that patient's best interest, because the consent is implied in the patient's need for medical intervention.

A situation where this comes into play is often in disclosing information to a patient's family, friends, and caregivers, especially in cases of overdoses. "This is usually used in cases where the patient's family, or whoever is helping them recover, needs information to help them find the next place for their care," Bowen says. "This was done to assist that patient in getting them help."

This is up to the physician's judgment. OCR has provided [guidelines](#) on what doctors are allowed to disclose specifically in these situations. OCR specifies that, for example, while a provider can use professional judgment to talk to the parents of a patient incapacitated by an opioid overdose about the overdose and related medical information, generally the provider could not share medical information unrelated to the overdose without permission.

Again, patient care is the provider's aim, and the minimum necessary information will be shared that is necessary for the continuation of care. HIPAA allows for CEs, like providers, to disclose information in cases where disclosing information may protect the patient or others from harm and the disclosure was made in good faith based on actual information they had at the time (see 45 *CFR* § 164.512(j)(4)).

Privacy, discrimination, and opioid use

OCR's announcement of an education program included nondiscrimination broadly, which can go hand-in-hand with privacy rights under HIPAA, especially for patients and families of patients with opioid use disorder and SMI. "The public needs to know that there should be no discriminatory actions to their access for assistance. If a facility receives federal funds, then they must allow equal opportunities for participation to their programs," says Bowen.

In a [press release](#) last year, **Roger Severino**, director of OCR, confirmed OCR's commitment to non-discrimination, particularly in the case of patients with opioid addiction. Severino pointed out that discrimination, bias, and stereotypical beliefs about persons recovering from opioid addiction can lead to unlawful barriers in accessing the healthcare and social services that are needed to address the opioid crisis.

The idea of stigma is echoed in a recent [blog post](#) by **George Sigounas MS, Ph.D.**, administrator of the Health Resources and Services Administration. "But one of the main focuses of the nation's fight against the opioid crisis is to fight the stigma that keeps people from seeking treatment, and health centers and community providers understand that as well as anyone. We're not sweeping it under the rug. We know that it doesn't matter the location, the economic status of the patient, the age, the gender - everybody's affected," he wrote.

Part of addressing stigma and discrimination, which can sometimes hold patients back from seeking treatment, is being aware of one's rights as a patient, and that includes the privacy protections of HIPAA. But HIPAA works in tandem with other laws to protect patients and encourage them to seek treatment.

Public health emergencies

Another situation where patients may need to know their privacy rights is in cases of public health emergencies like natural disasters. During the 2018 Atlantic hurricane season, for example, HHS Secretary **Alex Azar** declared such emergencies in areas heavily affected by the storms.

In general, a healthcare facility can call a disaster and then it is confirmed by state or federal authorities. In these cases, it means that the patient doesn't have to sign a consent form or authorization for information to be disclosed, explains Bowen. This includes the notice of privacy practices (NPP) that providers must make a good faith effort to get patients to acknowledge. However, as soon as the disaster is lifted, then providers must make a good faith effort to get those signed.

HHS and HIPAA allow for good faith disclosures of PHI in cases where public safety and patient safety demand it. A public health emergency allows physicians to share information on a case-by-case need, says Bowen. This extends to public health crises like the opioid crisis, which means information could be shared with other physicians to prevent patients from doctor-hopping or drug-hopping. "They have to enable physicians to share information through a health information exchange to notify other practitioners," she says.

Understanding state laws

A final privacy issue that patients need to be aware of is that HIPAA is not the only law protecting their privacy and disclosure. In addition to laws like 42 *CFR* Part 2, every state has laws in place that may be more stringent than HIPAA.

For CEs that do work in multiple states, this means they need to be aware of the differences in state laws and be prepared to clarify this information for patients. "All 50 states have unique rules for patient privacy, so it is imperative that the rules to mapped and the most stringent be applied," says Bowen. For patients, they need to know the law in the state where their healthcare provider practices.

Most states have privacy rules stronger than HIPAA, Bowen explains. HIPAA was written to be the minimum standard for privacy and security, and all 50 states have added more protections. Most states go beyond HIPAA in defining PHI that must be protected when it is health-related information as defined by the language of HIPAA.

HHS has provided [guidance](#) for questions where state laws differs from HIPAA, for example, when a state law is "contrary" to HIPAA, meaning it is impossible for a CE to comply with both (see 45 *CFR* 160.202). Generally, contrary state laws are preempted by federal requirements, unless an exception applies. The exceptions include if the state law:

- Relates to the privacy of individually identifiable health information and provides greater privacy protections or privacy rights with respect to such information.
- Provides for the reporting of disease or injury, child abuse, birth, or death, or for public health surveillance, investigation, or intervention.
- Requires certain health plan reporting, such as for management or financial audits. In these circumstances, a CE is not required to comply with a contrary provision of the Privacy Rule

The most important thing to convey to patients is that while there are nuances in the law, HIPAA is not meant to be a stumbling block to their receiving care. The primary purpose of HIPAA is to protect personal information from being shared outside routine healthcare operations. It is important for CEs to know the law, as well as other anti-discrimination laws, in order to assure patients that their safety and privacy are a top priority.