Are you a HIPAA entity? The "Privacy Law" is probably not what you think.

Terry A. Fletcher BS, CPC, CCC, CEMC, CCS, CCS-P, CMC, CMSCS, ACS-CA, SCP-CA, QMGC, QMCRC, QMPM
Healthcare Coding and Reimbursement Consultant and Auditor
NSCHBC Member
ICD10Monitor.com Editorial Advisory Board Member

If you have heard the acronym HIPAA thrown around a lot lately, you are probably thinking, "Do I really know what HIPAA means?". So many are throwing that term around in the falsehood that their legal or privacy rights are being violated in some way as more and more companies are requiring COVID-19 vaccines to secure employment, to stay employed, and now, let's face it to enter certain public places or to travel.

Well first, let's clear up the confusion.

The first thing you should know about HIPAA is that it's HIPAA, not HIPPA. There is only one P, and that P doesn't stand for "privacy."

"People make up what that acronym stands for," Deven McGraw, co-founder and chief regulatory officer of the medical records platform Citizen and former deputy director for health information privacy at the Department of Health and Human Services (HHS) Office for Civil Rights (OCR), had stated in a recent interview.

"More often than not, [they think it's] Health Information Privacy Protection Act: HIPPA. Yeah, that law does not exist.", McGraw said.

But now, we see the media asking government officials like Georgia Rep., Marjorie Taylor Green, or Dallas Cowboy quarterback Dak Prescott, or New England Patriots quarterback Cam Newton, all 'invoke" their HIPAA rights. Green even claimed, more than once, that just asking the question was somehow a "violation of her HIPAA rights". Incorrect. As more and more employers and healthcare entities and even schools, mandate that employees and students get vaccinated, we need to make sure we are clear on not only what HIPAA is, but how it is applied.

So let's get one big question out of the way first:

Is it a HIPAA violation for your employer to require vaccines?

No.

Nor is it a HIPAA violation for them to ask for proof that you have been vaccinated, though many people seem to think that providing or even soliciting any sort of health information automatically becomes a HIPAA issue.

Employers do have to keep their employees' vaccination statuses confidential, but that's because of the Americans with Disabilities Act — not HIPAA, which, again, doesn't apply here.

Why HIPAA is so misunderstood?

Both the misspelling and the widespread belief that HIPAA confers a strict set of privacy protections to any and all health data — and that everyone is subject to those laws — are common, although frustrating mistakes: Most patients only come across the term HIPAA, when signing the notice of privacy practices that the law mandates their health care providers have them sign. Plus, most people consider their health information to be very sensitive and assume their physicians and lawmakers have put the appropriate guardrails in place to keep it as private as possible. But HIPAA's privacy rules are more limited than many may realize.

What is not well understood about HIPAA, is its limits. It's very specifically a law that regulates information that is collected because a person is seeking health care.

Normally, the misunderstanding would be just an annoying misstep, but the pandemic has helped bring health privacy issues to the fore. As with many other things over the past year, we've moved many of our health interactions to the virtual space, and with the CMS 1135 Waiver flexibilities, under the C.A.R.E.S. Act, some of those interactions may not be covered or protected by HIPAA, but many people simply assume they are.

For example: If you are participating in a Telehealth encounter with your physician, and you are using a smart phone application, such as FaceTime or Skype, as allowed under the Waiver 1135 during the PHE, these platforms are not HIPAA protected, and your physician must inform you of that potential risk of breach of your personal health information, before you choose to continue with your visit. This also has to be well documented in the encounter that you were informed, in the way of consent.

What has happened since about 2-3 months into the pandemic, is that it has become increasingly politicized, and many people are cited "HIPAA rights" as an excuse to get out of mask mandates and to declare vaccine passports and mandates to be illegal. Neither of these assertions is true, but that hasn't stopped many people from making them — even though using them to avoid public safety measures could be harmful to everyone. People have such a high level of confidence believing misinformation, that it is out of control in the COVID era.

The perception that HIPAA is solely a health privacy law that everyone is subject to has become so common that there's a massive amount of confusion about who and what HIPAA actually applies to; that the sheer volume of bad information about it is nearly insurmountable.

Social media platforms have a been a problem, when attempting to give credible information. Trying to get people to understand what a "Covered Entity" or "Business Associate" is in 280 characters is not an easy task. These platforms can write the words, but of course, people will

believe what they want, and if it is contrary to what they want it to mean, then the platform doesn't lend itself well to a considered nuanced discussion.

What HIPAA actually does

So what does that one P stand for if not privacy? *Portability*.

HIPAA is short for the Health Insurance Portability and Accountability Act. The 1996 law's origins lie in creating federal standards for digitizing medical claims data and records ("accountability") and allowing employees to have health insurance coverage, including for preexisting conditions, when they changed jobs (that's the "portability") — rights they did not have before the Affordable Care Act.

The privacy provision, that most of us associate HIPAA with today, wasn't actually the focus of the law at the time. When Congress passed this law, they knew on some level, that there was going to be a massive digital transition to our health data in the future, and there might need to be privacy protections for that.

It took a few years to work those protections out, so HIPAA's privacy rules weren't issued until the end of 2000, and didn't fully take effect until 2002. There was a recent update in 2013.

HIPAA only applies to what are called "Covered Entities." Those are, essentially, health care providers (doctors, hospitals, and pharmacies, for instance), health insurers, and health care clearinghouses (which process medical data). It also covers their "business associates," or contractors who have to handle medical records in some way to do work for those covered entities. Those parties are required to follow certain protocols to keep your protected health information secure and private, especially in the digital transfer of patient health information.

This is why healthcare providers or insurers might require patients to communicate with them through secure, HIPAA-compliant channels and patient portals, or take other steps to verify a patient's identity before discussing protected health information with them. HIPAA's privacy rule also requires that health care providers give the patient, a notice of their privacy practices, and allow patients to access their own medical records. In fact, a lot of HIPAA complaints from patients aren't about privacy violations but about lack of access to medical records, which created the 21st Century Cures Act, to shift that focus to the OCR – Office of Civil Rights.

What HIPAA doesn't do

It's important to note that medical privacy didn't begin with HIPAA, and it's not the only health privacy law out there. The concept of doctor-patient confidentiality has existed for a long time — it's part of the Hippocratic Oath (which is not a law) — and that trust is a necessary part of good medical care.

Patients' have to feel a level of comfort that if they tell their personal physician some very private, and secret things, that they will be kept that way, and this allows a physician to give the patient the right care and diagnose them properly.

At the same time, many of people freely give away their health information to all kinds of places and platforms and to people who have no real legal obligation to keep that information private or secure. With the internet and social media, this is happening more than ever.

Consider this, If you're recording your steps on a Fitbit or you're using a nutrition app, that's not going to be covered by HIPAA. That is not a HIPAA entity and can use that information to market to you athletic shoes or equipment, supplements, etc.

That amazing massage therapist appointment you Tweeted about? Your vaccine card Instagram selfie? Your membership in a Facebook support group for people who have cancer? The period tracker app on your phone? The heart rate monitor on your wrist? Browsing WebMD for information about your recent COVID-19 diagnosis? The mail-order DNA test? The Uber trip you took to the emergency room? That is all health information, most of it is directly tied to you, and it can be sensitive, but none of it is covered by HIPAA (unless protected health information is shared with a covered entity, like a hospital or physician who ordered it, requested it, and asked you to deliver it that way. Even then, it is sketchy.

And then we've got the organizations that handle health data but aren't covered by HIPAA, including most schools, law enforcement, life insurers, and even employers. They may be covered by other privacy laws, but HIPAA isn't one of them.

A big hiccup to all this, is that we are still under the Federal PHE, (some states have let their PHE expire). So, some things that actually are covered by HIPAA have been given a temporary enforcement waiver due to the pandemic. The Office of Civil Rights will not be enforcing its rule requiring health care providers to use HIPAA-compliant portals for telehealth (as long as patients were informed), nor will it require covered entities to use HIPAA-compliant systems to schedule vaccines — an issue that arose when some health services' sign-up portals crashed and the services turned to the event scheduling platform, Eventbright. Eventbrite is a good service for getting a lot of people signed up for an event in high demand, but it's not HIPAA compliant, and posts events on a public forum.

The Office of Civil Rights (OCR) has stated that that enforcement discretion will remain in effect "until the Secretary of HHS determines that the public health emergency no longer exists, but again, patient's need to be informed of this security risk, as outlined in the CURES Act and the CMS FAQ rules sheets."

A Dose of Reality on HIPAA

Understand that if you go to Starbucks (not a covered entity) and refuse to wear a mask because you say you have a health condition, it is not a HIPAA violation if the barista asks you

what that condition is, nor is it a HIPAA violation if Starbucks refuses service to you. The are a private business and not a HIPAA entity and can enforce any rules they want that they feel protects public safety and their business, as long as it is not discriminatory to a protected class (i.e race, religion, gender, disability etc).

If your doctor were to walk into that Starbucks and broadcast your health information to anyone within earshot without your permission, *that* would be a HIPAA violation. It would also be a good time to consider changing doctors. Fortunately, HIPAA allows you to request your medical records and bring them to a new provider. And if someone else happened to record your doctor's outburst and put it on TikTok, *that's not* a HIPAA violation, even though it does include information that was once protected by HIPAA.

Additionally, someone asking if you've been vaccinated is not a HIPAA violation. In fact, it's not a HIPAA violation for anyone to ask about any health condition you may have, though it might be considered rude. A business requiring you to show proof that you've been vaccinated before you can enter is not a HIPAA violation. Your employer requiring you to be vaccinated and show proof before you can go to the office is not a HIPAA violation. Schools requiring that students get certain vaccinations before they're allowed to attend is not a HIPAA violation.

Oh, and vaccine passports — which the Biden administration has already said, it has no plans to mandate, but could change in the future – are also not HIPAA violations.

Look at certain health records apps that are all the rage now, like New York's Excelsior Pass (ePass) to use it, you are voluntarily giving the app permission to access your health records, and, as the app's disclaimer clearly states: "[T]he website is not provided to you by a health care provider, so, as such, you are not providing protected health information for health care treatment, payment, or operations (as defined under Health Insurance Portability and Accountability Act (HIPAA))." Does anyone read the fine print anymore?

So HIPAA isn't the all-inclusive health privacy law so many people assume it is, but that mass assumption suggests that such a law is both wanted and may be needed. HIPAA has a lot of gaps that a privacy law can and should fill. The pandemic has only made this more apparent.

What we need is for Congress to pass a comprehensive privacy law that sets limits on what the companies can use this data for, how long they can keep it, who they can disclose it to, and doesn't put the burden of dealing with that on the individual.

Rep. Suzan DelBene (D-WA) is one of several lawmakers who have pushed for better health privacy protections during the pandemic, including as a co-sponsor of the Public Health Emergency Privacy Act, a bill that was introduced in both houses of Congress in 2020 and reintroduced in early 2021. It's premise is that it would protect digital health data collected for the purpose of stopping the pandemic (for instance, by contact tracing apps or vaccine appointment booking tools) from being used for unrelated purposes by the government or private businesses.

HIPAA provides some protections for our health information, but technology has advanced must faster than our laws.

In the mean time, if you have any question whether or not you or another business or person is a "Covered Entity" and needs to comply with HIPAA standards, CMS has a tool to help health care providers and organizations determine whether or not they are considered a covered entity. The link is included below. Also, join me (Terry Fletcher) and Healthcare Attorney and fellow NSCHBC member, Amanda Waesch for our October 12th, episode of the NSCHBC Edge podcast. We will be discussing this very topic and diving into the legalities of these mandates and how it will affect healthcare providers in the near future.

References:

Notification of Enforcement Discretion for Telehealth | HHS.gov

HIPAA Covered Entity Decision Tool

Did you know that HIPAA (Health Insurance Portability and Accountability Act)-covered entities must also comply with standards for electronic transactions – not just privacy and security provisions? The Centers for Medicare & Medicaid Services (CMS) offers a tool to help health care providers and organizations check whether or not they are considered HIPAA-covered entities.

Visit the CMS Administrative Simplification website to learn about the standards and operating rules that are required for electronic health care transactions conducted by HIPAA-covered entities.