Is HIPAA Outdated? While Coverage Gaps and Growing Breaches Raise Industry Concern, Others Argue HIPAA is Still Effective

Save to myBoK

By Mary Butler

A Beverly Hills plastic surgeon, let's call him Dr. Hollywood, has a thriving business—an impeccable office, gracious and welcoming staff, and top of the line equipment and devices. His clientele is primarily celebrities and other wealthy socialites who can afford to pay out of pocket for cosmetic services, so Dr. Hollywood doesn't accept insurance. Occasionally, Dr. Hollywood gives interviews to celebrity magazines and talk shows commenting on specific patients of his and the work they've had done—naming names and discussing details.

Is this behavior unethical? Perhaps. Opportunistic? Definitely. But is it a HIPAA violation? No. HIPAA privacy rules only apply to covered entities, and strictly speaking, covered entities are considered as such because they exchange electronic information with health plans. So because Dr. Hollywood doesn't accept insurance, he is not a covered entity according to HIPAA. That said, his shady disclosures do put him in violation of California's stricter health privacy laws—and it is illogical gaps like these between state and federal law that have people questioning whether HIPAA needs an update.

Attorney Adam Greene, JD, a partner at the Washington, DC law firm Davis Wright Tremaine, says the plastic surgeon scenario is a classic example of the ways in which the public at large misunderstands the purpose of the 1996 HIPAA legislation and what it covers. And, he says, it's an example that even surprises people who've been working with HIPAA for years.

HIPAA is widely understood as a healthcare privacy law, but as Greene points out, the "P" in HIPAA doesn't stand for "privacy." The Health Insurance Portability and Accountability Act (HIPAA) was intended to make it easier for healthcare providers to transmit healthcare claims to health plans and clearinghouses using common standards. When HIPAA was being written, Congress took the position that if the law was going to facilitate greater electronic sharing of health information, there should be better privacy and security requirements that go with it.

"If you were drafting a health information privacy law it would likely be very different," Greene says. He adds that many privacy protections were added later through rulemaking, and that state privacy regulations followed to try and fill gaps.

HIPAA came of age at the same time as the Internet—though policymakers couldn't have foreseen how much the two developments would grow to impact each other. The Internet, of course, is the engine that has many in the industry pushing for more updates to HIPAA. Mobile health devices such as the FitBit, electronic health records (EHRs), telehealth services, social media, and other wearable health trackers have taken on a life of their own, outpacing privacy regulations—even with the HITECH update to HIPAA in 2009 and the Omnibus Rule changes in 2013—creating recent gaps in national privacy and security law. Some see this as a gap in HIPAA that should be filled.

Though it is over 20 years old, it appears HIPAA is still not completely understood by patients and providers. In 2016 the Office of the National Coordinator for Health IT (ONC) released a series of blog posts and fact sheets aimed at clarifying just what rights of information exchange and protection HIPAA grants patients and providers—in part to better foster the exchange of information that can become log-jammed over a misunderstanding of HIPAA's rules.

To determine whether HIPAA needs to be replaced or merely updated, it's important to hear from the privacy officers who work with its policies every day, current and former federal officials, and legal experts who work through patient issues and assist providers. Not all are in agreement that HIPAA is out of date. Some think it is still relevant and does a relatively good job of protecting privacy and security. Others think it should be scrapped and replaced with more modern and thorough regulation. All those interviewed for this article, however, agreed that at least some modifications and updates are called for.

Some Say Supplement HIPAA, Don't Replace It

It's tempting to believe that documents written before significant technological and scientific advances are automatically antiquated. Although people will likely debate key portions of the US Constitution forever, even skeptics agree that its core tenets have held up over time and served the country well. Similar consensus exists around HIPAA.

Greene, who counsels companies on HIPAA and HITECH compliance, says that HIPAA has also held up fairly well. And while technology has outpaced some of its provisions, HIPAA doesn't need to be altered to fill those gaps, Greene says, suggesting instead that other, newer privacy laws be created. "I think there's a danger in trying to extend HIPAA to other types of entities. HIPAA was designed very much with healthcare providers and health plans in mind. So just throwing a mobile app, a consumer-focused mobile app, into HIPAA is not necessarily the best fit," Green says.

Privacy officers interviewed for this article agree. Elisa Gorton, RHIA, CHPS, MAHSM, director of corporate responsibility, privacy officer, at St. Vincent's Medical Center in Connecticut, doesn't think the law needs to be broken down and rebuilt to become more relevant since its overall intention is very good. Gorton also thinks the Office for Civil Rights (OCR) does a good job with enforcing HIPAA. But, "It could probably be refreshed, because now you have telehealth going on and more patient portals, and more interactive types of care and communication done electronically. Patients want information texted to them… and we do have patients that want things e-mailed directly to them, and they don't want it encrypted or sent securely," Gorton says.

HIPAA Enforcement and Compliance is a Work in Progress

At a time when health information breaches are reaching an all-time high, HIPAA audits by the Office for Civil Rights (OCR) have continued in an attempt to make sure providers are following current privacy and security rules. According to Rachel Seeger, a spokesperson for OCR, Deven McGraw, deputy director for health information privacy at OCR, worked with a team of 18 people over this past year. This group was responsible for the HIPAA Privacy and Security Rule policy, overall enforcement monitoring, case reconsiderations, and more. They've been working with a budget projected to be $38.8 million, Seeger says.

"OCR has resolved over 24,825 HIPAA cases through corrective action and/or technical assistance since the agency began enforcing the Rules in 2003," Seeger said in an e-mail to the *Journal*. From September 2009 through January 31, 2017, OCR has received approximately 1,825 reports involving breaches of protected health information (PHI) affecting 500 or more individuals—with a total of 171,390,576 individuals impacted by these incidents. OCR has received approximately 255,560 reports of breaches of PHI affecting fewer than 500 individuals, according to Seeger.

That staff was certainly busy in 2016, a devastating year for HIPAA breaches. Over 25 million records were compromised as of October 2016 alone, according to *Fierce Healthcare*.[1] Such staggering numbers have some questioning the effectiveness of OCR's audits and the PHI protections required in HIPAA.

While privacy and security breaches seem to be getting worse, some have defended OCR's efforts to combat incidents. Increased enforcement in the recent year—long awaited OCR "desk audits" started in 2016—have been praised.

Regarding these desk audits, attorney Adam Greene, JD, admits, "Nothing is ever quite enough to ensure all the providers are going to follow up… the audit program has definitely had a substantial impact in pushing more covered entities and business associates to prioritize HIPAA compliance, and admittedly everyone's got limited resources…," Greene says. "The alternative is more of a traffic ticket mentality and penalizing everyone that is found to have violated HIPAA, but I prefer the current approach."

Kelly McLendon, RHIA, CHPS, managing director at CompliancePro Solutions, says that even the small number of desk audits do a good job of "sowing a little bit of fear, certainty, and doubt that 'Hey, I could get audited—I'd better be compliant,'" he says.

McLendon admits that with thousands of covered entities and business associates eligible to be audited, the chances for the average organization to be one of the 150 chosen by OCR is "microscopic." But that doesn't mean organizations shouldn't be prepared anyway. "Being prepared for the audit is also being prepared for an investigation, which could come at any time,

based on a patient making a complaint… You're at risk even if your risk of audit is very small. Your risk of having to produce all that information [for an audit or investigation] is not all that small," McLendon says.

Nancy Davis, MS, RHIA, CHPS, director of compliance and safety at Door County Medical Center, admits that while technology is always changing, the philosophy that drives HIPAA is "fairly sound." However, she would welcome "more clarification on patient portals." Davis also says, "HIPAA does tend to defer to state law when it comes to minors. So that's always a challenge."

And it does appear that regulators are hearing industry calls for HIPAA updates. In remarks delivered at the HIMSS Annual Meeting in February, Deven McGraw, JD, MPH, deputy director for health information privacy at OCR, said her agency is expecting to release a draft rule on privacy breaches by the end of 2017. McGraw noted that HITECH requires the Department of Health and Human Services (HHS) to devise avenues for compensating individuals whose healthcare privacy has been breached—and that may happen soon.

"What qualifies as harm when there has been a violation of privacy and security rules? How do we determine a violation has occurred when the case is settled and there is no finding of fault?... We'll be issuing that [proposed rule] hopefully in 2017," McGraw said, according to a report in *Medpage Today*.[2]

Additionally, OCR will issue guidance on topics such as text messaging—including when and how it's appropriate to send text messages containing PHI using unsecured texting platforms. The guidance will also speak to permitted uses and disclosures of PHI on social media platforms—another update some in the industry have said is needed to bring HIPAA into the 21st century.

McGraw also said OCR is working on guidance she's termed "Anatomy of a Case," which "walks through a typical case we do in HIPAA and how we calculate penalties, and the basic criteria we use to come to settlement amounts," said McGraw, according to *Medpage*.

Gaps Between State and Federal Privacy Laws

State laws around protected health information (PHI) often are much more stringent than federal law—since HIPAA is often called the floor of privacy protections, not the ceiling—and it's the privacy officer's job to be familiar with both. Some in the industry have called on replacing HIPAA with an updated, overarching, national privacy and security law governing all PHI that would serve as the regulation ceiling. Davis admits that having to consult one overriding privacy law instead of several would make life easier.

"I would relish one set of laws. In a perfect world, HIPAA would be the end-all—no separate set of rules for minors or mental health. The three biggest areas that I struggle with are law enforcement, minors, and reporting drug diversion," Davis says.

"In Wisconsin, the laws to protect patient privacy are stronger than HIPAA when it comes to reporting and sharing information with law enforcement. We always hear from law enforcement, 'HIPAA says we can do this.' And I say 'That's true HIPAA does, but it's your Wisconsin law I'm following.' So yeah, it would be nice to have one set of laws, but I don't see that happening because there are a lot of political issues" at play, Davis says.

But privacy and security consultant Joy Pritts, JD, the former chief privacy officer at ONC, looks at the discrepancy between state and federal law differently. She feels stricter state law helped improve HIPAA over the years, leading to HIPAA updates in 2003 and 2009 that added privacy and security protections first modeled at the state level.

"I have a philosophical perspective on that, based on years of watching how laws develop in the United States, and I really do believe that if you didn't allow the states to do something in this area, we wouldn't be where we are today. We would not have breach notification in HIPAA if states had not started breach notifications—California in particular. I'm not in favor of federal preemption of state law because that's where a lot of the good ideas originate," Pritts says.

Stakeholders are worried about gaps in HIPAA falling short of protecting consumer data as patients access PHI through mobile health and patient portals. The government has also expressed concern. Last year ONC addressed these concerns with

a report called "Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA."[3] The report analyzed the current scope of HIPAA; identified gaps that exist between HIPAA-regulated entities and those not regulated by HIPAA; and makes recommendations for leveling the playing field for innovators that are covered entities and non-covered entities (NCEs). It also assessed the role of the Federal Trade Commission (FTC) in protecting health data.

The paper stated that HHS has committed to providing more guidance for providers of technologies offered by NCEs, as well as for entities that are unsure whether they are covered by HIPAA.

The paper ultimately concluded that "large gaps in policies around access, security, and privacy continue, and confusion persists among both consumers and innovators. Wearable fitness trackers, health social media, and mobile health apps are premised on the idea of consumer engagement. However, our laws and regulations have not kept pace with these new technologies. This Report identifies the lack of clear guidance around consumer access to, and privacy and security of, health information collected, shared, and used by NCEs," the report concluded.

How to Make HIPAA Work Better

While there is consensus that HIPAA and its updates have held up over time, there are a diverse set of ideas various stakeholders have for tweaking it or pushing for privacy protections in other places.

Pritts says that in an ideal world, all organizations—from HIPAA-covered entities to app developers—that handle health information would have codes of conduct that would be enforceable by the FTC. Pritts thinks that HIPAA is very prescriptive in that it covers a segment of organizations that handle health information in a certain way while not covering others—like Dr. Hollywood.

"And outside of that context, we have hardly any protection. What I see as being an issue is there's such a difference between HIPAA and the Federal Trade Commission Act," Pritts says.

For example, according to the ONC report, the "FTC and HHS each have broad experience in protecting consumers against privacy and security risks to health data to the extent of their existing statutory authorities... FTC has a well-developed body of law enforcing privacy and security practices that are unfair and deceptive, including taking action against an organization that adopts a code of conduct, but does not adhere to that code. HHS' experience includes well-established regulations about health data privacy and security, as well as in-depth knowledge of the ways that very sensitive data moves (and will move in the future) among FDA-regulated devices, EHRs, mHealth apps connecting into medical environments, and the emerging connectivity among them in health care delivery settings. As this Report shows, however, large gaps in policies around access, security, and privacy continue, and confusion persists among both consumers and innovators."

"It's not just a question of does HIPAA need to be fixed or improved, it's whether regulatory structure needs to be improved," Pritts says. "That's what I would focus on personally and in doing that I would make it a little more uniform between the kinds of sensitive information that's covered by HIPAA and what's covered by the FTC."

Pritts says she would like one "overarching privacy rule that would go a long way in the US toward evening out the discrepancies between health information and other types of information," though she also admitted that the practical political realities render that somewhat unrealistic. However, she says work on privacy will continue. "We're never going to be done in this area. It's evolving constantly and we do need to keep up with the way data is generated and exchanged," she says.

One problem that persists with HIPAA is that the technical and legal language can be hard for consumers and professionals to interpret. AHIMA's Privacy and Security Practice Council is working to improve patient understanding by developing a form to accompany the Notice of Privacy Practices (NPP) form that patients fill out for their doctors. This form, meant to explain to consumers how an organization protects their privacy, is often very complex—and has been ridiculed by some consumer advocates as unreadable and unhelpful to consumers.

"That is an area where I think we could step back and try to do better, which is not only educating providers but also simplifying some of their requirements. That's especially important when you're looking at how people access their health

information now," Pritts says. "Many have moved to mobile devices, iPads, and tablets. Having a very long NPP that's not in a paper format doesn't really work. An authorization that is very, very long doesn't really work either."

Lucia Savage, JD, who most recently served in the Obama Administration as ONC's chief privacy officer, worked on the ONC blog series and fact sheets that attempted to clear up some of the consumer and provider confusion about HIPAA.

One of the biggest challenges of modernizing HIPAA is that consumers are ready to "go mobile" in the delivery and receipt of their health information but many providers still are not, Savage says. Even with the guidance ONC and OCR have released, patients are too frequently told that they can't have their own health information or get it exchanged with other providers. One reason for this is that there are many moving parts.

"We've done a really excellent job of raising the awareness of the importance of privacy among healthcare professionals and office managers, a really excellent job. But in this particular case, we maybe overcorrected," Savage says. "We need to swing the pendulum back a little bit. For a patient to be told 'I can't give you information about you,' it just doesn't hold up to scrutiny. And that's different than you saying as a professional 'I don't have authorization to send this to your husband's divorce attorney so I'm not going to,' which is completely legit."

Pritts and Savage agree that providers need more training and education around the release of information through patient portals. "I think that providers do need more information. There's been a big push for consumers to have more access to their own information and patient-generated data. From my interactions with major healthcare systems, even they are not familiar with the [Omnibus] rule that came out in 2013 that said individuals have the right to designate a third party to receive their information under a right of access request," Pritts says.

Improved patient access to their own information—as well as information exchanged between providers—may be best achieved outside of HIPAA or new regulations. Private industry—some with the help of government grants and some without—are making great strides in secure information release.

For example, last fall ONC announced the winners of its "blockchain challenge," which required participants to explain how blockchain technology could enable interoperability. Blockchain is a technology that was first used to protect Bitcoin currency transactions, but interoperability experts believe it's also a promising way to exchange sensitive health information in a private and secure way. Software developers are also using application programming interfaces (APIs) to develop tools that make patient information stored in EHRs more readily available to patients.

Pritts currently sits on the board of advisors for a company that's working on ways to make information, like PHI, easier to send securely.

"They [the company] are enabling granular control of information in a way where you don't have to be concerned whether state A has one law or state D has another law," says Pritts, alluding to discrepancies in state privacy laws.

One way to improve security without touching HIPAA or issuing a regulation could be by letting innovators innovate. "I think, to me, the best course is to really have competition for the best in class and let the consumer pick what's right for them," Savage says.

Notes

[1] Hirsch, Marla Durben. "2016 a banner year for EHR security breaches." *Fierce Healthcare*. December 29, 2016.

[2] Frieden, Joyce. "HHS Eyes End of 2017 for Draft Rule on Privacy Breaches." *Medpage Today*. February 20, 2017.

[3] Department of Health and Human Services. "Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA." June 17, 2016.

Mary Butler (mary.butler@ahima.org) is associate editor at the Journal of AHIMA.

Article citation:
Butler, Mary. "Is HIPAA Outdated? While Coverage Gaps and Growing Breaches Raise Industry Concern, Others Argue HIPAA is Still Effective" *Journal of AHIMA* 88, no.4 (April 2017): 14-17,52.

Driving the Power of Knowledge

Copyright 2022 by The American Health Information Management Association. All Rights Reserved.