A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

COMPLIANCE TODAY MAGAZINE

APRIL 2026

CINDY MATSON
VICE PRESIDENT, COMPLIANCE AND AUDIT SERVICES AT SANFORD HEALTH

THE POWER OF RELATIONSHIPS AND TRUST IN COMPLIANCE (P6)

30 Years HCCA®

CCB article click for CEU quiz

THINKING ABOUT HEALTHCARE PRIVACY IN 2026

by Kirk J. Nahra

Kirk J. Nahra
(kirk.nahra@wilmerhale.com) is a Partner and Co-Chair of Cybersecurity and Privacy Practice with WilmerHale in Washington, DC.

Privacy and security law for the healthcare industry has never been more confusing. It's never been easy; the HIPAA principles governing most healthcare privacy issues for many years are complicated, so much so that many people can't even spell HIPAA (and even fewer really understand what it does). In recent years, even this relative simplicity has disappeared, making the field much more confusing and complicated and raising real risks that privacy confusion will get in the way of an effective healthcare system. Coupled with ongoing data security risks and the growth of AI opportunities in healthcare, these challenges are growing rather than shrinking, creating meaningful and challenging compliance risks across the healthcare ecosystem.

We aren't sure what health information means anymore

U.S. privacy law—and, really, privacy law everywhere—has always treated healthcare information differently from other kinds of information. In the EU, health data is considered "sensitive" data—but so is whether you are a member of a trade union. U.S. law is both more nuanced and more complicated. The core privacy principles of the HIPAA Privacy Rule—once you get past all of the interrelated cross references and definitions—protect essentially every piece of personal information that a healthcare provider or a health plan has about an individual if that individual is their patient or insured. This means your heart rate and diabetes status, as well as your name, address, phone number, and email, are available to the impacted business if it has this information because you are their consumer. So, HIPAA focuses

mainly on *who* has your data rather than what the data is.

We are seeing new state laws defining healthcare information in various ways. We see some of the new "consumer health" privacy laws (such as the My Health My Data Act in Washington) include not only clearly identifiable health information, but also your location in certain contexts and data that can lead to inferences about your health. If this law were in effect in Washington, DC, where I work, it would protect my location data as "health" data when I sit at my desk at my law firm, type my emails, and make Zoom calls—because the George Washington University Hospital is next door to my building. If a pharma company wanted to contact me for a clinical trial because I am a white male of a certain age, the "inference" about that information would relate to my potential health status for the study, making this kind of outreach highly risky.

In other situations, we have clearly identifiable health data, such as information about ankle surgery after an athletic injury. If that information is about me after a tennis injury, few people care. If it is LeBron James and he won't play in the NBA again, everyone cares; it's not because of an ankle injury, but because it's LeBron James. So, this "sensitivity" relates to who the data is about—not what the data itself is. This is before we even get to social determinants of health, where we know that your zip code, your proximity to good food, and your housing status matters for your health. We know that children living in certain areas face educational difficulties due to the health impacts of pollution on their brains. We are aware that what a young girl watches on TikTok can impact her mental health and eating disorders. So, it's getting very hard to evaluate what "health information" means in a way that makes special regulation of this category useful (at some point, it's just going to be all data that exists about you).

There are conflicts between policy goals

We are also seeing more tensions between "privacy" goals and other goals of the healthcare system. Various state laws are being passed in the wake of the *Dobbs v. Jackson Women's Health Organization* decision. Some of these laws—one in California, for example—essentially require segregation of reproductive rights information from the rest of the medical record. This may provide certain protections for a California woman caught up in an abortion investigation. At the same time, it creates gaps in medical records, impacting almost any woman in California. The Washington law makes it harder to recruit specific patients for clinical trials. We know that one risk of AI is bias in complex datasets. Privacy law is making it harder to find people who can counterbalance this bias. And we are seeing certain regulators (for example, the former chair of the Federal Trade Commission) asserting that certain kinds of data—such as health data—should not be used to train AI models at all, or that certain additional "consent" is needed from individuals before their data should be used for AI (for an analysis of why this position would be bad for consumers and the healthcare system, see endnote 1).[1] If this approach is adopted, either we won't have AI in healthcare (not a likely outcome), or, if consent is mandated, we can expect these bias concerns to be exacerbated, as different groups are likely to opt out in unexpected ways. These competing considerations are one reason healthcare privacy is so hard. If you regulate how data about my purchases at the Gap can be used and disclosed, not too many people care all that much. But healthcare privacy impacts a wide range of stakeholders: the government as regulator, providers and payers, taxpayers overall, employers, and individuals across a range of settings.

It's getting very hard to evaluate what 'health information' means in a way that makes special regulation of this category useful.

Security in the healthcare system remains a problem

Another area of tension involves the security of healthcare data. We continue to see large and small security breaches impacting health information, within the HIPAA framework and beyond. Part of what drives these security issues is the need for the healthcare system to enable broad data sharing—and the related policy goal of allowing patients to have greater access

to their own healthcare data. When a patient gains access to their own data from multiple healthcare providers, that data "leaves" HIPAA's protections and moves into a largely unregulated space controlled by the patient. To allow doctors to view medical records while on the golf course or otherwise away from the office, we need broad, mobile access. To meet the requirements of the new information blocking rules, data must be provided to a wide range of audiences with essentially assumed appropriate purposes. So, security remains a challenge in the healthcare system, at least in part because of these goals about broad accessibility.

At the same time, more and more state breach notification laws apply to health information. It is challenging to see the purpose of some of these requirements. If a company has a breach involving your Social Security number, it is required to tell you about it because there are things that you can do to protect yourself. For your healthcare information, it's much harder to see the point: "Dear patient, The information about your ankle surgery was stolen by a hacker. Accordingly, you should (do what exactly?)." Coupled with the range of entities involved in the healthcare system—from solo practice doctors in rural areas to some of the largest companies in the country and vendors of every size and shape—we can expect security to remain a problem in search of an appropriate solution for the foreseeable future.

New law is creating confusion (with even more likely to come)

Adding to this complexity is the wide range of new laws impacting healthcare privacy. There are state laws in virtually every state providing specific rules for certain kinds of health information (often called "sensitive condition" laws). There are also federal rules—such as the Part 2 substance abuse rules—providing similar unique provisions (and also creating broader healthcare concerns about appropriate treatment because of specific restrictions that make treating certain conditions harder). There are "comprehensive" privacy laws in 20 states (so far) that apply to a lot of health data outside the scope of HIPAA, whether or not it's treated as a separate category of sensitive data. We have consumer health laws in several states (such as the Washington law previously discussed), with likely more to follow (we expect a New

York consumer health privacy law in 2026). While these laws (primarily) are well-intentioned, they may not appropriately factor in other healthcare policy goals, *and* they are leading to a growing complexity in the broadest healthcare ecosystem. This confusion means there is no rational basis for consumers to understand the rules, and it is also increasingly hard for healthcare businesses to understand their obligations. That doesn't seem good for anyone (well, except me, as a healthcare privacy lawyer). It is likely that this confusion will grow in 2026 as more laws are passed at the state level (there was an important federal consumer health proposal introduced in late 2025, but passage is unlikely; for an analysis of this new federal proposal, see endnote 2).[2]

National legislation isn't likely to solve any of these problems

In addition, aside from the small likelihood of a national privacy law passing this year, I would expect any such law (if the proposals from the past few years are any guide) to actually make this problem of complicated healthcare privacy rules worse rather than better. Fundamentally, all of these "comprehensive" proposals would exempt entities covered by existing law, particularly the HIPAA rules. So, rather than creating any kind of uniformity in the law, this national proposal would likely simply add another layer of complexity to the already unwieldy health privacy structure. I blame the healthcare industry in part for this status—the position of a broad swath of the healthcare industry in the national privacy law debate is "leave us alone, we have HIPAA." That means that the people who know the most about these issues are largely sitting out the debate. Other entities—largely the tech companies—are not fully cognizant of the challenges in healthcare, and they have other fish to fry in this debate. So, healthcare is given little separate consideration, leading to this unfortunate likely result.

Conclusion

Data is central to an effective and efficient healthcare system. Without data, we cannot evaluate health trends, identify new treatments, or evaluate the system's effectiveness for patients. This data is about people—usually, specific identifiable people who care about the privacy of their information. These privacy rights need to be protected; however, simultaneously, we also need to ensure that the healthcare system can work effectively for the benefit of both patients and the healthcare industry (and all other relevant stakeholders). The current developments in this body of law are making compliance more difficult and increasing the risk that this critical balance will not be met, to the detriment of both patients and the healthcare industry. CT

Endnotes

1. Kirk J. Nahra, "Regulator Concerns and the Benefits of AI in Health Care," *The SciTech Lawyer* 21, no. 2 (Winter 2025): 4–11, https://www.wilmerhale.com/-/media/files/shared_content/editorial/publications/documents/20250228-the-scitech-lawyer---regulator-concerns-and-the-benefits-of-ai-in-health-care.pdf.
2. Kirk Nahra, "Trying to make sense of health privacy," IAPP, November 25, 2025, https://iapp.org/news/a/trying-to-make-sense-of-health-privacy.

Takeaways

- Healthcare privacy law is growing more complex as HIPAA's entity-based model collides with expansive state consumer health laws and evolving definitions of "health information."
- New state laws increasingly treat location data, inferred data, and social determinants as health data, making nearly all personal data potentially subject to heightened regulation.
- Privacy protections now conflict with other health system goals, including clinical research, AI bias mitigation, complete medical records, and effective care coordination.
- Data security remains fragile as broad data sharing, patient access, mobile use, and information blocking rules expand exposure beyond HIPAA's traditional safeguards.
- Fragmented state laws and unlikely federal solutions are increasing compliance confusion, risking an imbalance between privacy protection and the data-driven needs of effective healthcare.