20 March 2025
OPINION

Subscribe to Newsletters →
Advertise with the IAPP →

Health Care | North America | Law & Regulation | Enforcement

Why health care privacy is a mess — and why it isn't likely to get better soon

Related stories

- A view from DC: New York readies to pass an extraordinary health privacy law
- The state of US reproductive privacy in 2025: Trends and operational considerations
- HHS proposes major overhaul of HIPAA security rule
- US courts, regulators weigh in on online tracking in health care
- Online tracking technologies and HIPAA misconceptions

Kirk Nahra
Contributor
CIPP/US
10 Minute Read

Editor's note: The IAPP is policy neutral. We publish contributed opinion and analysis pieces to enable our members to hear a broad spectrum of views in our domains.

Since the early 2000s, health care privacy has mainly meant the Health Insurance Portability and Accountability Act. This has always been a little misleading.

The HIPAA statute focused on health insurance portability and standard electronic transactions, with privacy mainly an undefined afterthought. It was clear at the time that the HIPAA privacy rule crafted by the Department of Health and Human Services was of important but limited applicability. It applied to specific entities, those involved in portability and standard transactions, for certain information in certain situations. It was never intended as an overall health information privacy law.

Even then, HIPAA applied on top of an existing body of health privacy laws. There were state laws in virtually all states applicable to specific health conditions — almost all passed before HIPAA when there was no applicable federal framework. There was also a federal substance abuse information law — again passed in a different policy environment without an existing federal privacy framework and where the primary goal was to ensure law enforcement did not learn of an individual's treatment for substance abuse because of the risk of prosecution for drug use.

HIPAA then became the core federal baseline where it applied. It was drafted by HHS — because there was no substantive policy direction from Congress — to balance two critical policy goals. It was designed to provide strong privacy protections for regulated personal information and to permit and facilitate an effective and efficient health care system that benefits patients as well as the health care industry.

Where HIPAA applies, it generally works well. Both covered entities, mainly health care providers and health insurers, and patients generally support its protections and provisions. These rules also did an excellent job overall of considering privacy on a broader level — how it fit in with other public policy goals — so privacy did not become "the only" point in the discussion.

Since the HIPAA privacy era began in the early 2000s, as the industry adapted to the HIPAA requirements, we also saw a critical additional development: the massive expansion of non-HIPAA health data. This, at the time, largely unregulated data created real concerns. Health information generally is perceived as sensitive data, and there are substantial concerns about how it can be misused without a specific regulatory framework.

At the same time, there was also a substantial expansion of thoughts around what health data is. Laws and regulations began to develop to address both topics. In recent years, the tears in the structure have grown and created both tensions on privacy protection and unnecessary complexity for the health care system, making it much more difficult to develop a strong overall system. And in the past few years these challenges have exploded to the point where health care privacy now is a mess.

Growth in non-HIPAA data

We have always known about the existence of non-HIPAA health data, meaning data related in some reasonable way to health information but not regulated by HIPAA because of the limited scope of the law itself.

In the early days this meant insurers outside health insurance, such as auto, life, disability or workers' compensation, and

employers in the normal course of employer activities, like job applications, doctors' notes, and Family Medical Leave Act, Americans with Disabilities Act and workers' compensation claims.

These are certainly important issues and data, but they are likely to be regulated in some other way or are not really the source of most major concerns in privacy.

But in the last dozen years or so, the data in this unregulated space has exploded. It is mobile apps. It is wearable technologies. It is health information websites. It is personal health records. It is patient support groups around the country. And it is most of the data tech companies collect in the normal course of their business, like posts on Facebook about an upcoming surgery, Google searches and Twitter inquiries.

Lots of specific health information, which may or may not be about a specific individual, is mostly unregulated and is certainly not regulated by HIPAA.

Overlapping laws

As a result of HIPAA gaps and other societal developments, we are seeing more and more laws that may cover some of this non-HIPAA data, as well as perhaps the HIPAA data itself. Both Texas and California have HIPAA-like laws that apply to both HIPAA entities and a broad range of others, with language mirroring HIPAA's rules even where this may make little sense.

As a lawyer who spends a lot of time on these issues, it is virtually impossible to make sense of these laws. Questions include whether a HIPAA-covered entity or business associate has to do something different or not and how other kinds of covered companies can make sense of a law that is largely written to apply to doctors and hospitals.

We are seeing enormous growth in state comprehensive privacy laws, which clearly cover wide ranges of health data, mostly outside HIPAA. Laws like the Maryland Online Data Privacy Act are creating substantial challenges before health information can be used for virtually any purpose, developing an approach to consumer consent that is essentially the opposite of what HIPAA requires.

And then there are the laws prompted by other issues, for example Washington state's My Health My Data Act was driven by the Dobbs decision but applies far beyond reproductive rights information. There are unintended consequences in areas like clinical trials and medical research, where the law is making it harder to find appropriate patients for clinical trials, particularly from diverse audiences.

And there is a different Dobbs-related law in California, which despite admirable goals, may in some instances harm women's health more broadly by requiring segregation of reproductive rights information from the rest of the medical record.

So, we are seeing multiple laws impacting the same date depending on the specific role it plays in a particular context.

New FTC and state regulatory activity

The U.S. Federal Trade Commission is also acting to fill some of these gaps, although this development likely will be slowed or halted in the new administration. Because the FTC doesn't have specific laws on health care issues, it has been targeting activity related to health data it finds problematic, either as an unfair practice or as an unauthorized practice triggering the otherwise unused Health Breach Notification Rule. This has included taking enforcement action in cases based on a revised interpretation of the regulatory language well before it was actually revised to say what the FTC believed it said.

We have seen similar enforcement activity at the state level. State attorneys general, recognizing the gaps in the law, have used their overall consumer protection authority to define appropriate activity in the health care space but without specific useful rules on what principles companies should follow in the first instance.

These actions have led to tremendous uncertainty in the digital health area. While I am often skeptical of claims that regulatory and legislative activity impedes innovation, these actions clearly made it challenging to enter new digital spaces in health care, despite the enormous need for new health products.

No clarity on what health data means anymore

In parallel, while it is gospel to say health information deserves additional privacy protections, a broad range of new developments now make it highly challenging to identify what health information actually is. When a law protects location data of those near a health care facility, is that really health information? Is it always health information? Does it mean anything at all in the normal course? When medical researchers reach conclusions based on voting patterns and television viewing habits and shopping trends, is that health data?

We understand why specific kinds of medical data deserve extensive protection, such as an HIV diagnosis, substance abuse treatment or mental health issues. Does the same need apply to information about your ankle surgery? Is my ankle surgery after a tennis injury the same as Lebron James' ankle information if it means he won't ever play basketball again?

Some of the new laws, like Washington state's MHMDA, apply to inferences about health, leading a wide range of companies who do not believe they have health data — and who don't in most situations — to now need to consider these laws.

Could federal legislation help?

Congress has been debating a national privacy law for more than 20 years with no success to date. How would this law — if it ever were to come into effect — impact this mess? Sadly, even if there were to be a national privacy law, it likely would not help this situation and might even make it worse.

All the federal proposals that have received any meaningful attention have carved out those entities subject to HIPAA from their coverage. This means there would at least be two sets of rules in the health care industry. Many preemption proposals also exempt state health privacy laws, meaning this confusing new set of laws would actually remain in effect.

In addition, because the core health care industry supports the exemption of HIPAA entities from this law, the primary discussion on health privacy, which has not been a focus of attention, involves primarily entities and businesses that are not the primary users of health care information and have other priorities.

There is not enough thinking going into this highly complicated area. So, a federal law, if we ever get one, is likely to make things worse rather than better.

Why does this matter?

The HIPAA privacy rules, drafted entirely for policy reasons beyond the statutory limitations on who was subject to the laws, did a thoughtful and thorough job of considering broad public policy considerations along with creating important privacy protections.

We are not seeing the same thoughtfulness in the chaotically developing law at this point. This legal complexity is creating challenges for medical research at a time when medicine is becoming even more personalized and the need to add diverse populations to research protocols is growing.

Public health is being challenged, as data restrictions for one purpose are impacting our ability to protect the public health. Numerous studies following the COVID-19 pandemic bemoaned the lack of data about COVID activity, where many of these limitations were driven by short-term privacy considerations.

We are also seeing nervousness about artificial intelligence perhaps leading to overregulation in the health care field, which may mean AI does not become potentially valuable for the health care industry and the patient population it serves.

The health care system relies on data, mostly data about people. When it is too confusing or risky to use this data, the health care system and the patients it serves suffer.

Conclusions

I hope to raise these issues for broader consideration but do not have a magic bullet. The current situation — particularly because of new state laws addressing a number of related topics where there are unintended consequences — is likely to continue, making this situation worse, in the short term at least.

Long term, we are missing a thoughtful way to address these issues overall. The HIPAA rules, which are not perfect but do

engage in this thoughtful balancing, could serve as a model, particularly in areas like the approach to consent. But there is currently no viable mechanism to turn this thinking into public policy.

We are not likely in the short term to see cohesive thought on these issues at a federal level. We could see some of this thinking at the state level, but leading states seem to be focusing on specific isolated goals rather than evaluating broader systemic concerns. I encourage public policy advocates to become involved in these issues, but there typically have been more immediate and direct issues taking their attention. The same is true of the privacy academic community, where the leading thinkers are focused primarily on broader privacy issues rather than an integrated evaluation of linking privacy with broader health care concerns.

We need more attention on these issues overall. We are all and will continue to be patients, and we need effective privacy along with the best health care system we can have.

Kirk Nahra, CIPP/US, is a partner at WilmerHale in Washington, D.C., and co-chair of the firm's cybersecurity and privacy practice as well as its artificial intelligence practice.
