January 30, 2021 01:00 AM

Patient privacy laws are due for an overhaul, experts say

MICHAEL BRADY

Getty Images

The Health Insurance Portability and Accountability Act—HIPAA—turns 25 years old in August, and experts say it's time for the patient privacy law to finally live up to its promise.

While HIPAA mostly succeeded in safeguarding patient health information created in the healthcare system, it hasn't enabled widespread information sharing and doesn't really protect health-relevant information outside the traditional healthcare system.

Most experts agreed the nation’s health privacy rules are long overdue for an overhaul, given all the changes that have taken place in healthcare and technology since 1996, though some insiders think the current regulatory system works well enough.

CMS in December unveiled proposed changes to HIPAA regulations to ramp up information sharing. The measures have ample support from providers, health plans, technology vendors and privacy experts. But there’s a growing need for more robust protection of patient health

information and health-relevant data to ensure industry stakeholders can successfully use digital data to improve patient outcomes.

The proposed rule aims to achieve two key goals: give patients more control over their data while at the same time make it easier for clinicians to share patient data with other providers, insurers and social service agencies for coordinating patient care. Experts say the plan would help shift providers' mindset from protecting patient health information to sharing it, which was HIPAA's original goal.

Those changes were in line with the Trump administration's focus on ensuring regulations don't stand in the way of patients being able to access their health information, with updates like shortening the period in which covered entities' are required to respond to patients' record requests from 30 to 15 days. The rule builds on the "Right of Access Initiative" that HHS' Office for Civil Rights announced last year, as well as former HHS Deputy Secretary Eric Hargan's push to eliminate barriers to coordinated care. It also aligns with the Office of the National Coordinator for Health Information Technology's recent rule regulating interoperability and information blocking.

It’s unclear whether the Biden administration will move forward with the proposals, although several of the planned changes have bipartisan support.

SUBSTANCE ABUSE PRIVACY REGULATIONS STRICTER THAN HIPAA

While HIPAA enables healthcare providers and payers to share significantly more information than many people recognize, federal privacy rules governing substance abuse disorder diagnosis and treatment are still very restrictive, said Manatt Health partner Randi Seigel.

She said many health plans and providers take an overly cautious approach to sharing such information because they don’t want to violate the rules, which carry significant penalties.

For a long time there have been calls for updates to the substance abuse disorder privacy law, 42 CFR Part 2, to align it with HIPAA, said former CMS official Lisa Bari, a healthcare consultant and interim CEO of the Strategic Health Information Exchange Collaborative. “Some small, technical actions have been taken, but there’s still this huge gap and chasm there,” she said. “And states and other entities are trying to make it work, but it’s still not totally clear.”

HIPAA changes needed

Many in the industry are arguing it’s time for Congress to update the HIPAA law to meet the healthcare system’s changing needs. “There isn’t any way for any administration to just, through regulation, expand the coverage of HIPAA to cover more health data than it currently covers. They’re hemmed in by the statute,” said former HHS official Deven McGraw, now chief regulatory officer for data-sharing startup Ciitizen.

Quarles & Brady partner Meghan O’Connor would like HIPAA to better account for changes in how personal health information is collected, stored, transferred, processed and

governed because it's grown increasingly complex since Congress wrote the law. She said the statute doesn't sufficiently address cloud services, telehealth platforms and other technologies and services that have emerged since Congress enacted it more than two decades ago. "HIPAA treats each covered entity and business associate as an island or a silo. That's just not really how health information technology works anymore. It's not (just) information collected by the provider and stored on a computer or some kind of system that's entirely owned and controlled by a provider," O'Connor said.

HIPAA mandates that covered entities have contracts—called business associate agreements—with their vendors explaining privacy and security requirements. It also requires every subsequent agreement to have the same privacy and security protections as the original contract between the HIPPA-covered entity and the initial vendor. "It makes sense in theory," O'Connor said, but doesn't work in practice because there are so many cloud services, platform vendors and other intermediaries involved. "It's not feasible that everyone is going to renegotiate contracts with Microsoft or Google … each time they sign a new contract with a hospital," she said.

Sidley Austin partner Colleen Brown said policymakers could be more likely to scrutinize downstream vendors in the future since they're particularly vulnerable to cybersecurity attacks and more likely to misuse health information.

The American Hospital Association declined to comment for this story.

An outdated approach

The existing regulatory framework is "not adequate because HIPAA was originally designed to facilitate the sharing of health information and … since that time there have been multiple updates to HIPAA to reflect the changing landscape (but) we don't see that health information is flowing as needed, even with patient consent," said former CMS official Lisa Bari, a consultant and interim CEO of the Strategic Health Information Exchange Collaborative, which includes 81 HIEs nationwide.

She noted that Congress ordered regulators to create new rules on interoperability and information-blocking in the 21st Century Cures Act to make it easier for providers, insurers and patients to exchange health data—mostly by requiring providers and insurers to adopt standardized application programming interfaces that connect IT systems like electronic health records with third-party apps. "That seems

a little ridiculous. Doesn't it? That you would have to pass a different law and write different regulations to stop something that, on its surface, should be facilitated by HIPAA. It's not meeting the needs of today and what's happening on the ground," Bari said.

The new interoperability, info-blocking and HIPAA rules are an opportunity to make healthcare more data-driven.

But as more and more data begins to flow, policymakers will have to figure out how to regulate patient health information as it moves in and out of HIPAA-covered entities, such as when a patient connects their EHRs to an app like Apple Health.

Once that information leaves a HIPAA-covered entity, the Federal Trade Commission is mainly responsible for making sure it's not misused.

Dr. Kenneth Mandl, director of the computational health informatics program at Boston Children's Hospital, said the agency could enforce an app's terms of service and end-user license agreement to privacy. But it might be challenging for regulators to take action since those terms aren't standardized across apps and offer varying degrees of consumer protection.

Insiders are also concerned about personal health information losing its HIPAA protection once it's stripped of all personally identifying information because there's a substantial risk that someone could still identify patients using sophisticated techniques like combining anonymized health records with other data sets. There are no clear consumer protections against re-identification in the U.S., except in California.

HIPAA also doesn't safeguard health-relevant data created outside the healthcare system. For example, people with poor credit histories are less likely to adhere to their medication regime than people with good credit profiles. Providers, insurers or third-party apps could use such information to help people better adhere to their medications. But an accountable care organization or Medicare Advantage plan could use that information to exclude some people "because they're not going to provide the outcomes that you're hoping for from a healthcare or financial perspective," Mandl said.

Experts worry that regulators won't keep up with enforcement as more and more people share their personal health information with an ever-growing number of apps. Agencies like the FTC often lack the resources needed to enforce the rules, an issue that seems likely to intensify.

Types of health-relevant information

Most people think HIPAA only applies to data generated by hospitals and healthcare systems, but it actually covers a wide range of data if a HIPAA-covered entity holds it. Still, most health-relevant data like internet search histories goes mostly unprotected because it usually lives outside HIPAA-covered entities like health plans.

Data source	Examples
Healthcare system	Electronic medical record data, prescriptions, laboratory data, pathology images, radiography, payer claims data.
Consumer health and wellness industry	Wearable fitness tracking devices, medical wearables such as insulin pumps and pacemakers, medical or health monitoring apps, patient-reported outcome surveys, direct-to-consumer tests (including DNA analysis) and treatments.
Digital exhaust that's a byproduct of a consumer's daily activities	Social media posts, internet search histories, location and proximity data.
Non-health	Race, gender, income, credit history,

demographics, social and economic sources	employment status, education level, residential ZIP code, housing status, census records, bankruptcy and other financial records, grocery store purchases, fitness club memberships, voter registration.

Source: npj Digital Medicine (2021) 2

Some think HIPAA works

But Sidley Austin's Brown said the proposed rule shows that federal regulators have enough tools to ensure that HIPAA can change with the times, even though Congress hasn't significantly revised the law since 1996. Not only did OCR make significant policy changes, it also clarified what HIPAA already allowed to clear up confusion among providers and payers. Brown noted that federal regulators frequently offer guidance to ensure providers and payers know how to apply HIPAA as technology advances and the healthcare system changes.

Moreover, the FTC and other federal agencies have the power to regulate health-relevant information that isn't covered by HIPAA. For example, the FTC can go after companies for unfair or deceptive practices. "For the most part, people recognize that the HIPAA regime is important and should be largely retained," Brown said.

Other experts agreed that it makes sense to have specific rules to protect patient health information created by the

healthcare system because that's more sensitive than health-relevant information like data from fitness trackers.

States take action

Another barrier to health information sharing is that almost every state has its own set of privacy rules. Some state privacy regulations mirror HIPAA, while others are more restrictive. Several states also have laws protecting information about specific types of treatment like behavioral health. "Navigating those state rules, especially if you're a multistate provider or health plan, can be really challenging," Manatt Health partner Randi Seigel said.

The list of state rules that providers, payers and technology vendors must navigate is growing longer each year, as states have taken it upon themselves to tackle privacy and data-sharing issues that Congress hasn't taken up yet. The California Consumer Privacy Act of 2018 gives consumers broad data privacy rights, including protections for biometric data and health insurance information. It has a special carve-out to preserve HIPAA's protections for personal health information. States like Illinois, Texas and Washington have also passed privacy legislation specific to biometric information, while many others are considering general data privacy laws similar to California's.

The different regulatory approaches and definitions have created a web of confusing and intersecting rules to navigate. That's led many health plans and providers to resist sharing health-related information because they're worried about breaking state rules.

Federal action needed

It's time for Congress to pass new legislation to deal with the recent and coming changes in technology and the healthcare system, according to most experts.

In addition to modernizing HIPAA, insiders said standardizing how states regulate patient health information could increase information sharing by giving insurers and providers more clarity about what the law allows. Congress could revise the law to prevent states from creating more restrictive rules through federal preemption—a legal doctrine under which federal laws supersede conflicting state laws. That would establish a common, nationwide standard for HIPAA-covered entities to follow. But it would also prevent state policymakers from increasing protections, even if they thought it was necessary.

Experts acknowledged that state experiments could help policymakers discover best practices for safeguarding health-relevant data. But most of them supported new

federal legislation to protect information that isn't covered by HIPAA because it would make data sharing more manageable and more likely.

Although many experts want Congress to create a general data privacy law like California's, others say it makes more sense for lawmakers to develop privacy laws that address particular industries because it's unlikely that a standard set of rules would meet everyone's needs. Yet it could prove challenging for policymakers to devise industry-specific privacy rules as technologies and industries evolve, intersect and overlap.

Co-leader of Manatt's privacy and data security practice Scott Lashway supported a sector-specific approach, saying it would be a "mistake" if Congress tried to regulate health information based on its views of social media companies and data breaches. Both issues seem to drive lawmakers' interest in data regulation.

A new law focused on health-relevant data might be easier for Congress to pass since it would only require one or two congressional committees to move through the legislative process. A general data privacy law would require several committees to sign off.

“It’s always easier for Congress to focus on a sector because that’s the way they’re organized in terms of committee structure, staff expertise and things of that nature,” Ciitizen’s McGraw said. She supports a general privacy law, but thinks healthcare-specific legislation is needed.

Broader protections sought

Insiders said there’s a growing consensus that the nation’s privacy laws need an update, and it seems more likely to occur now that Democrats control the White House and both chambers of Congress. “I think there is a bipartisan appetite for it (because) of how big tech is handling our information in general,” said Sen. Bill Cassidy (R-La.), a physician who has cosponsored several privacy bills. He thinks Congress could update health privacy laws in the next few years, but it will take time to figure out how to deal with the necessary trade-offs between privacy and freer data sharing.

According to an article by McGraw and Mandl, most of the bills Congress is considering have significant shortcomings because they rely too much on notice and consent and overvalue de-identification, among other issues. “But it would be a shame if we didn’t advance healthcare to the

level of other industries in terms of the use of data for intelligence, improvement and discovery," Mandl said.

RELATED ARTICLE

Data Points: Enforcing HIPAA

Letter to the Editor

Send us a letter

Have an opinion about this story? **Click here to submit a Letter to the Editor**, and we may publish it in print.