dataprotectionlaw&policy
Volume: 10 Issue: 2

Analysing the US HIPAA legacy and future changes on the horizon

The US Department of Health and Human Services issued the long-awaited final omnibus rule under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) on 17 January 2013, which has set a federal level baseline for US healthcare privacy. Kirk Nahra, Partner at Wiley Rein LLP discusses the evolving landscape of privacy in this industry after 40 years of legislative and political history.

Introduction

The core healthcare privacy system in the US works reasonably well. The HIPAA regulations, which have been the primary driver of privacy protection for a decade, provide the foundation principles in most situations. However, even these rules reflect both inconsistent internal approaches and an evolving attention to particular goals, and therefore often provide little assistance or overall confidence in more difficult situations. At the same time, they do not control a wide variety of situations involving healthcare privacy, which other laws - particularly state laws - may control, or no law controls.

We see, therefore, an ongoing sense of calm and normalcy in the mainstream, combined with ongoing challenges, confusion and often counterproductive demands and requirements, for more difficult, complicated or emerging situations. And, with each passing regulation or law, we see a movement towards more confusion and controversy, rather than less.

Background

For many decades, healthcare privacy protection in the US was driven exclusively by professional ethics, primarily for healthcare providers, and a mosaic of state privacy laws. There was no consistent federal baseline standard. There are thousands of state laws and regulations that provide privacy protection for specific kinds of healthcare information in particular situations. It is virtually impossible to catalog all of them (although many have tried), and any reasonable effort at comprehension leads to a conclusion that the laws do not fit together in any reasonable way, nor are they consistent or practical or readily understandable by any of the affected entities (including the core question of who is even covered by many of these laws).

Enter the HIPAA regulations. The HIPAA era began with the passage of the Health Insurance Portability and Accountability Act in 1996. While HIPAA now

means many things to many people, at its foundation, the HIPAA law focused on 'portability' - the idea that individuals could take their health insurance coverage from one employer to the next, without having pre-existing health conditions acting as an impediment to job transitions.

When Congress passed HIPAA, it also added into the mix a variety of other topics related to the healthcare industry, such as creating large funding for what has now become an extended fight against healthcare fraud. One of the policy mandates adopted in HIPAA was to move toward standardized electronic transactions for the healthcare industry. The idea was that certain 'standard transactions', such as the submission of a health insurance claim and the payment of that claim, could be standardized and thereby, create efficiency savings and more effective results. With these standardized transactions came a concern about healthcare information being put into electronic form, with the resulting requirements for the creation of the HIPAA Privacy Rule and the HIPAA Security Rule.

But this background also led to one key component of these rules: the limits on the applicability of these rules to 'covered entities' - such as doctors, hospitals and health insurers who might be participating in these standardized transactions. The law mandated the rules, but restricted their application to those covered entities only. That means that a large number of entities who obtain or use healthcare information are not within the scope of these rules, such as consumer-facing entities, many healthcare websites, life and disability insurers, employers in their employment role, etc.

Due to this limitation to covered entities, HHS developed a creative solution to respond to a key fact about the healthcare system. While the covered entities are core participants in the industry, they rely on tens of thousands of vendors to provide them services, with many of these services involving patient information. Therefore, the concept of a 'business associate' was born – an entity that provides services to the healthcare industry where the performance of those services involves the use or disclosure of patient information.

Because HHS had no direct jurisdiction over these 'business associates', HHS imposed an obligation on the covered entities to implement specific contracts with these vendors that would create contractual privacy and security obligations for these vendors. The failure to execute a contract would mean that the covered entity violated the HIPAA rules. A business associate's failure to meet a contractual privacy standard would be a breach of that contract, but would not subject the business associate to government enforcement, because the business associate was not regulated under the HIPAA rules. This system has existed since the inception of the HIPAA Privacy Rule in 2003.

Now, we have round two of the HIPAA regulations, driven largely by Congress, with some additional assistance and incremental additions by the applicable regulatory agency, which we are only beginning to review, analyze and

implement. After almost four years, the Department of Health and Human Services finally has released its omnibus HIPAA/HITECH regulation, implementing changes to the HIPAA Privacy, Security and Enforcement Rules, as well as the interim final regulation on breach notification and certain changes to the Privacy Rule as required by the Genetic Information Nondiscrimination Act (GINA Act). The regulation was published in the Federal Register on January 25, 2013.

These changes result from the 2009 passage of the HITECH Act. The schizophrenic nature of the HITECH law has been well documented. Simply put, Congress desired to incentivize - meaning pay - healthcare providers to implement electronic health record systems. Congress decided that:

- it would impose new privacy compliance obligations on those who chose to use electronic health records; and
- then would create a new set of privacy obligations for everyone else, unconnected in any way to the use of these electronic health records.

This statute reflected an ongoing mix of priorities. Congress 'fixed' one of the key gaps of the original legislation and rules, by applying the enforcement reach of HIPAA to not only covered entities but their 'business associates' as well. (In the final regulation, HHS extended this to downstream contractors of the business associates as well). It increased the available penalties for HIPAA violations, cut down on permitted marketing, and modified and expanded certain individual rights.

Even with its recent expansion, HIPAA is still not a general medical privacy law. While its scope has broadened, its protections still depend on where healthcare information starts, with a healthcare provider or health plan. That leaves enormous gaps in protection, particularly given recent technological and philosophical developments that are encouraging consumer involvement in their own healthcare and providing the technology to make this goal a reality. Although this legislation does not turn business associates into covered entities, it does impose - for the first time - direct accountability on these business associates, with potential civil and criminal liability for a failure to meet these requirements. But aside from some modest clarifications (such as ensuring that health information exchanges are treated as business associates), the HITECH law did not fundamentally broaden the overall HIPAA scheme, nor did it address in any way the tensions between HIPAA and the thousands of applicable state laws.

Ongoing Concerns

This structure leads to a variety of ongoing tensions that affect the efficiency of the healthcare system, the effectiveness of individual privacy and the operations of the overall healthcare system, including the systemic benefits of large scale data analysis.

Single rule vs. Multiple rules

HIPAA sets a federal floor, but states can pass 'more stringent' laws protecting individual privacy. The difficulty is often in reconciling whether a law is more stringent or not. This often leads to enormous confusion, particularly where actions can be taken but are not because of confusion over the laws. The prominent school shooting at Virginia Tech several years ago resulted in some widespread attention to how confusion among many affected professionals (doctors, psychiatrists, teachers, administrators, etc.) led to less information about the individual being shared than was permitted. This ongoing confusion leads directly to the question of whether a more straightforward, EU-type rule would benefit both individuals and businesses, by leading to clearer rules, and more efficient and effective activities.

Research

With technological advances, there are enormous opportunities for medical research, based on the volume of data and the movement towards electronic data. Yet, the HIPAA rules create significant limitations on how research can be conducted and have been heavily criticized by many in the research community. The new HIPAA rules take some modest steps towards eliminating some of these research impediments, but there clearly is room for more.

Technology vs. security

There continues to be an ongoing tension between the opportunities of technology and the risks of security breaches. Modest examples include providing individuals with electronic access to their records while still protecting security, but is becoming much more focused because of mobile technology and applications for healthcare activities. This dilemma is highlighted because so many mobile applications are consumer-driven, meaning that there may be no 'covered entity' to dictate any regulatory requirements.

Health information exchanges

The idea of these health information exchanges is to make medical information more available, leading to broader reliability of data, better treatment and fewer mistakes, while also improving efficiency and the opportunity for research and public health benefits. Yet these systems - which are being designed at a state or even local level by numerous parallel groups - are being driven by state law privacy concerns that dictate what information can and cannot be included in these records. To the extent that records are incomplete, it is hard to see how these goals will be met.

Solutions

So, the healthcare privacy model in the US is a work in progress. The progress is slow, while the movement of technology is fast. Are there ways to improve this system? What are the viable options?

Do nothing different

HIPAA works most of the time. Where state law provides a different result, people have largely been working things out. And other agencies, such as the Federal Trade Commission (FTC), are moving to fill in some of the gaps in scope.

Pre-empt (replace) state law

While HIPAA pre-empts weaker state laws, it permits existing laws that are more stringent. Because most of these laws were written pre-HIPAA, use different language and have wildly different approaches, these state laws create confusion and controversy along with their additional protections. A step that pre-empted all state laws would help, particularly with Health Information Exchange organizations ('HIEs'), but might (in limited circumstances) reduce certain protections (although these may be mainly theoretical).

Pre-empt existing state law, permit future laws

A variation on this pre-emption approach would be to pre-empt all state laws currently in place, but permit states to pass future laws with more stringent protections. This would eliminate the thousands of laws that are in place now, with all of the uncertainty they create. Most of these laws will not be replaced. And, where new laws are passed, they could be tailored to the HIPAA model so that it is much easier to tell what the rules are and to whom they apply.

Expand HIPAA to broader medical information

HIPAA could also be broadened (independent of these pre-emption issues) to apply to a broader range of healthcare entities (or entities that receive or use healthcare information). This would broaden the reach of the baseline standards, but might create other concerns where the HIPAA principles don't exactly fit other circumstances.

Healthcare data protection outside HIPAA

The creation of other vehicles to protect healthcare data is happening slowly, both through legislation and through enforcement activity (by the FTC and state Attorneys General). There are modest efforts in Congress to create general federal privacy or information security laws. The likelihood of passage is not

great. These laws, if applied to 'non-HIPAA' healthcare data would provide additional protections beyond what exist today. It would be a mistake, however, to create additional regulation for the entities that currently must follow the HIPAA rules.

Conclusion

The healthcare privacy efforts in the US create many rights and protections for individuals, and create significant compliance obligations for the healthcare industry and its core service providers. The system generally works well, but it is important to understand both where it works and where it doesn't, and to think about meaningful ways to improve the overall structure. A better healthcare privacy system would in fact benefit individuals, healthcare business and the system on the whole, but we are a long way away from solving this wide variety of issues.

Kirk Nahra
Partner
Wiley Rein LLP
knahra@wileyrein.com
