Kirk Nahra Publishes Two-Part Healthcare Privacy Series in The Privacy Advisor, a Publication of the International Association of Privacy Professionals

FEBRUARY 5, 2020

By Kirk J. Nahra

Partner Kirk Nahra recently authored a two-part article published by the International Association of Privacy Professionals. In the first installment, Kirk explores how we got to where we are today with health care privacy. In the second part of the series, he assesses options for moving forward to address emerging gaps and an evolving health care industry.

This article originally appeared in The Privacy Advisor, a publication of the International Association of Privacy Professionals.

Part One: GDPR, CCPA's Potential Impact on Federal Health Care Privacy

In the U.S., we do not, today, have a national privacy law. Pressure from the EU, via the General Data Protection Regulation, and from California, via the California Consumer Privacy Act, are driving an extensive national debate on this topic. But how is this pressure impacting the health care industry, both today and going forward? This two-part series will first explore how we got to where we are today with health care privacy. The second installment, in the next edition of The Privacy Advisor, will assess options for moving forward to address emerging gaps and an evolving health care industry.

So far, health care data may not be getting enough attention in the debate, driven (in part) by the sense of many that health care privacy already has been addressed. Due to the odd legislative history of the Health Insurance Portability and Accountability Act, however, we are seeing the implications of a law that was driven by considerations not involving privacy and security and also

reflected a concept of an industry that no longer reflects how the health care system works today. Accordingly, we are faced with a growing volume of “non-HIPAA health data” across enormous segments of our economy and the challenge of figuring out how to address concerns about this data in a system where there is no specific regulation of this data today.

The substantial history behind the HIPAA experience to date also provides meaningful insight into how a future privacy law could work. There are critical elements of HIPAA that have worked well — for both consumers and industry — and from which we may take lessons for the future. At the same time, the gaps in HIPAA’s protections — mainly the result of a legislative accident and significant technological and industry change — have grown to largely untenable levels. How is health care data being addressed today? How can we begin a dialogue on how these principles should be applied to protect consumers while at the same time permit the critical health care industry to move forward effectively and efficiently?

Setting the stage

The HIPAA Privacy Rule has set the standard for the privacy of health care information in the U.S. since the rule went into effect in 2003. Despite criticism from various directions, it has fundamentally reshaped the privacy and security environment for the health care industry.

Yet, from the beginning, the HIPAA Privacy Rule has had important gaps. The Privacy Rule was the result of a series of Congressional judgments about “scope" and driven by issues having nothing to do with privacy, like the “portability” of health insurance coverage and the transmission of standardized electronic transactions. As a result of the HIPAA statute, the Department of Health and Human Services only had the authority to write a privacy rule focused on HIPAA “covered entities” (health care providers, health plans and health care clearinghouses). Meaning, certain segments of relevant industries that regularly use or create health care information were not within the reach of the HIPAA rules. Therefore, the HIPAA Privacy Rule has always been a “limited scope” privacy rule. Bound by the statutory framework, the Privacy Rule focuses on “who” had your health care information rather than the information itself.

While these gaps existed from the beginning, most components of the traditional health care industry were covered by the HIPAA rules. What has changed in recent years is the enormous range of entities that create, use and disclose health care information outside of the reach of the HIPAA rules. We have reached (and passed) a tipping point on this issue, such that there is enormous concern about how this “non-HIPAA” health care data is being addressed and how the privacy interests of individuals are being protected (if at all) for this “non-HIPAA” health care data.

So, what exactly is the problem?

Because of the limited scope of the HIPAA statute, a broad range of entities that collect, analyze and disclose personal health information are not regulated by the HIPAA rules. For example,

numerous websites gather and distribute health care information without the involvement of a covered entity (meaning that these websites are not covered by the HIPAA Privacy Rule). We have seen a significant expansion of mobile applications directed to health care data or offered in connection with health information or overall wellness. The entire concept of "wearables" post-dates the HIPAA rules and generally fall outside the scope of HIPAA. Unless a HIPAA-covered entity is involved, these activities are generally outside of the scope of the HIPAA Privacy Rule and subject to few explicit privacy requirements (other than general principles such as the idea that you must follow what you say in a privacy notice).

In addition, as “patient engagement” becomes an important theme of health care reform, there is increased concern about how patients view such uses of data and whether there are meaningful ways for patients to understand how their data is being used. The complexity of the regulatory structure (where protections depend on sources of data rather than “kind” of data) and difficulty of determining data sources (which are often difficult, if not impossible, to determine) has led to an increased call for broader but simplified regulation of health care data overall. We see meaningful situations across the health care spectrum that involve data protected by HIPAA at one point and then, through permitted disclosures, no longer receives the protections of the HIPAA rules. These growing gaps call into question the lines that were drawn by the HIPAA statute and easily could lead to a reevaluation of the overall HIPAA framework.

What can we learn from the HIPAA model?

For better or worse, the core elements of the HIPAA rules can be summarized as follows. HIPAA incorporates a specific set of "covered entities," those companies (or perhaps individuals) directly subject to the law. By defining a set of regulated entities, HIPAA is typical of the sector-specific U.S. approach to privacy law. It then incorporates a means of addressing service providers (first by contract, then by law after legislative change).

One of the key choices in the development of the HIPAA rules — one that some say could be enormously useful model in the development of a national privacy law — involves the approach to consumer consent and related ability of these covered entities to use and disclose regulated information. The idea of “consent” under HIPAA is straightforward: Consent is presumed for certain key areas for uses and disclosures of personal information tied to “normal” operations of the health care industry. For this set of purposes — treatment, payment and health care operations — consent is presumed under the law. This defined set of “permitted” purposes is tied both to “normal” activities that we want to encourage in the health care system (for the benefit of all health care stakeholders) and effective operations of the health care system, consistent with consumer expectations.

The HIPAA rules also permit disclosures for certain “public policy purposes” (think public health and regulatory investigations), where consumer consent is viewed as not directly relevant. All other uses and disclosures are permitted only with explicit patient permission.

The HIPAA rules incorporate a series of individual rights (with a continuing focus on the importance of access to the consumer's information). There are a series of administrative requirements. HIPAA includes a separate set of security principles and breach notification rule. There is primary civil enforcement through the HHS Office for Civil Rights, potential criminal enforcement through the Department of Justice, and parallel civil enforcement through state attorneys general. There is no private right of action.

With this background on the HIPAA rules today, the next part of this two-part series will review alternative options for the regulation of health care data and assess how these choices may develop in the ongoing national privacy law debate.

Part Two: How Emerging Privacy Laws Are Impacting the Health Care Industry

This second installment assesses options for moving forward to address emerging gaps and an evolving health care industry. Why? Because the substantial history behind the Health Insurance Portability and Accountability Act experience to date also provides meaningful insight into how a future privacy law could work.

Health care in the national privacy law: Today's debate

While the Health Insurance Portability and Accountability Act creates the current baseline for privacy regulation of health information, how else can the privacy of health care information be addressed? Other regimes have chosen different approaches to health care privacy.

GDPR

The EU General Data Protection Regulation takes a very different approach than HIPAA. Under the GDPR, health information is treated as sensitive data, but there are no specific requirements for the health care industry per se. The GDPR is, therefore, both broader and narrower than HIPAA in its approach. It applies to more kinds of entities that have or use health information, but applies to less information than if that information were held in the U.S. by a covered entity (for example, a name or Social Security number held by a U.S. hospital is protected by HIPAA, while such information would not be health information under the GDPR). There is additional consideration in the GDPR of the health care industry on its own.

California's Confidentiality of Medical Information Act

Some states have their own laws that mirror HIPAA to some extent. (Technically, HIPAA sets a federal floor for privacy protection. It preempts weaker state laws but permits "more stringent" laws that provide greater privacy protections.) California, for example, has the Confidentiality of Medical Information Act. This is a freestanding law — different from the CCPA — that is parallel to HIPAA; it

clearly includes many HIPAA-covered entities and business associates, but also includes additional entities that are not subject to HIPAA, primarily entities providing mobile apps or other health technology directly to consumers. It is extremely challenging, to say the least, to evaluate the differences between HIPAA and CMIA for HIPAA-covered entities (and very difficult to apply the law to other kinds of entities that appear to be subject to it).

California Consumer Privacy Act

Then, since California is not confusing enough for health care, we now superimpose the California Consumer Privacy Act on the existing structure. As a general matter, CCPA exempts entities covered by HIPAA. It exempts covered entities for any HIPAA-covered data and business associates for their HIPAA activities. Intriguingly, it also exempts entities covered by the CMIA. The CCPA does seem to cover certain medical information that is held by entities that are not subject to HIPAA or the CMIA. Presumably, the collective approach in California covers all health care information in some way (with the potential exception of certain employer-collected health information not subject to HIPAA). The CCPA, however, is emphasizing the challenges for an industry that now regularly crosses the lines for these different laws.

Federal concepts so far

At the federal level, we are starting to see a variety of approaches to the overall question of national privacy legislation. While health care has not recently been a focus of this debate, each approach has its own perspective on health care and health information, along with its own strengths and weaknesses.

The Protecting Personal Health Data Act, proposed by Sen. Amy Klobuchar, D-Minn., is the only current legislative proposal that focuses on the issue of “non-HIPAA health data.” It creates a focused solution to the “scope” problems left by HIPAA’s tortured legislative history but only takes a “first step” approach to a solution by requiring a task force and then regulations “to help strengthen privacy and security protections for consumers’ personal health data … collected ... by consumer devices.” It targets this current gap but would not create a uniform set of rules across the industry, as we would still have different rules for HIPAA and non-HIPAA data.

Other approaches are more general and take varying approaches to how a new law would intersect with HIPAA. Sen. Ron Wyden's, D-Ore., Consumer Data Protection Act is mainly focused on expanding and increasing Federal Trade Commission authority without addressing health data directly. Another approach, Sen. Brian Schatz's, D-Hawaii, Data Care Act of 2018, defines “sensitive data” to include health care data. Unlike other proposals, the obligations seem to be superimposed on top of HIPAA (similar to the approach of the Sen. Ed Markey, D-Mass., privacy proposal, the Privacy Bill of Rights Act).

Sen. Marco Rubio's, R-Fla., proposed "American Data Dissemination Act" includes medical history and biometric as categories of data subject to the law but not health data overall. It generally exempts entities subject to HIPAA and preempts state law. In the House of Representatives, Rep.Suzan DelBene, D-Wash., has introduced "The Information Transparency & Personal Data Control Act." This proposal creates a wide range of obligations related to "sensitive personal information," including health information, but does not otherwise address the health care industry per se. These provisions appear to be imposed on top of HIPAA, and there is an explicit carve-out from the preemption provision for state laws that are more stringent than HIPAA.

Where are we now?

We can expect significant debate over the next few years on the future of a federal privacy law. While it might be possible for a health care "fix" to move separately, that seems unlikely at this point.

In thinking about the "gaps" in the current HIPAA structure, there are several options. Moving from "most limited" to "broadest" in application, we could see specific proposals approaching this issue in the following ways:

A specific set of principles applicable only to "non-HIPAA health care data" (with an obvious ambiguity about what "health care data" would mean).

- A set of principles (through an amendment to the scope of HIPAA or some new law) that would apply to all health care data.
- A broader general privacy law that would apply to all personal data (with or without a carve-out for data currently covered by the HIPAA rules), with recognition that it is increasingly difficult to identify "health care information."

In parallel consideration, a national privacy law could:

- Exempt the health care industry to the extent regulated by HIPAA.
- Include new provisions that apply to HIPAA covered entities, in addition to the existing HIPAA provisions.
- Replace HIPAA with a new structure covering all health care information.

At a minimum, we can expect that any new national privacy law would "cover" "non-HIPAA health care data" (and entities). But, unless a broader approach to health information is taken, that would continue the status quo of different standards depending on who is holding the health information.

Despite the importance of the health care industry, HIPAA and health information to the overall debate about individual privacy, health care has not been a leading factor in the current national

privacy legislative debate. This is unfortunate and can lead to problems for both the health care industry and a variety of other stakeholders interested in health care data and the privacy of this data. The HIPAA rules — because of their detail and our broad experience with them over the past 15 years — can provide some useful experience in evaluating the national debate (particularly in HIPAA's approach to consent and the use and disclosure of covered information).

In general, most relevant stakeholders are comfortable with the HIPAA approach and overall impact of the rules on the operation of the health care industry and the protection of patient data. Despite this comfort, the health care industry and these other stakeholders (including government, employers, researchers, patients and general consumers) need to consider what the next phase of privacy protection for health information should be. The current status quo — where the protection of health information depends dramatically on who holds the information — likely may persist in a national privacy law setting. That has important implications for consumers and for the health care industry. These differing standards create confusion and complexity that easily could be reduced through a common standard.

The health care industry, those in Congress and other relevant stakeholders should be evaluating whether a common standard, even if different from HIPAA, would be better for the industry and for consumers.