WILMERHALE

WILMER CUTLER PICKERING HALE AND DORR LLP

Reprinted with Permission from the *ABA Health eSource*

Healthcare in the National Privacy Law Debate

By Kirk J. Nahra, Esq., the ABA Health eSource, Vol. 16, No.4, December 2019 --

Kirk Nahra

Congress is debating whether to enact a national privacy law. Such a law would upend the approach that has been taken so far in connection with privacy law in the United States, which has either been sector specific (healthcare, financial services, education) or has addressed specific practices (telemarketing, email marketing, data gathering from children). The United States does not, today, have a national privacy law. Pressure from the European Union's General Data Protection Regulation (GDPR)[1] and from California, through the California Consumer Privacy Act (CCPA),[2] are driving some of this national debate.

The conventional wisdom is that, while the United States is moving towards this legislation, there is still a long way to go. Part of this debate is a significant disagreement about many of the core provisions of what would go into this law, including (but clearly not limited to) how to treat healthcare — either as a category of data or as an industry.

So far, healthcare data may not be getting enough attention in the debate, driven (in part) by the sense of many that healthcare privacy already has been addressed. Due to the odd legislative history of the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[3] however, we are seeing the implications of a law that (1) was driven by considerations not involving privacy and security, and (2) reflected a concept of an industry that no longer reflects how the healthcare system works today. Accordingly, there is a growing volume of "non-HIPAA health data," across enormous segments of the 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. These gaps have led to a broad range of entities that create, use, and disclose healthcare information outside of the reach of the HIPAA Rules. This growing range of non-HIPAA health data needs to be addressed in some way.

This leads to the national debate. There are a variety of approaches that are being applied today to healthcare. This article will explore some of the models to date, and reviews other efforts to provide standards for the treatment of healthcare data. In addition, this article will look at a new challenge — the usefulness of data that does not seem to be about our health in the healthcare industry. The primary goal of this article is to identify these issues and begin (or, to be fair, continue) a

dialogue (although one that has largely stalled and then been taken over by the broader national privacy law debate) on how these principles should be applied to protect consumers while at the same time permit the critical healthcare industry to move forward effectively and efficiently.

Setting the Stage

The HIPAA Privacy Rule[4] has set the standard for the privacy of healthcare information in the United States since the Rule went into effect in 2003. Despite criticism from various directions, it has fundamentally reshaped the privacy and security environment for the healthcare industry by creating a set of national baseline standards across the healthcare 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," driven by issues having nothing to do with privacy, such as the portability of health insurance coverage and the transmission of standardized electronic transactions. As a result of the HIPAA statute, the U.S. Department of Health and Human Services (HHS) only had the authority to write a privacy rule focused on HIPAA "covered entities" (healthcare providers, health plans and healthcare clearinghouses) — meaning that certain segments of relevant industries that regularly use or create healthcare information, such as life insurers or workers compensation carriers, were not within the reach of the HIPAA Rules. Therefore, the HIPAA Privacy Rule and the other HIPAA Rules have always been "limited scope" Rules, rather than a general health information privacy regulation. Bound by the statutory framework, the Privacy Rule focuses on "who" had one's healthcare information rather than the information itself.[5]

In the beginning, while critical gaps certainly existed, these gaps were somewhat limited, and large components of the healthcare industry — including most healthcare providers and health insurers — were covered by the HIPAA Rules. What has changed in recent years is the enormous range of entities that create, use, and disclose healthcare information outside of the reach of the HIPAA Rules. The system now has reached (and passed) a tipping point on this issue, such that there is enormous concern about how this "non-HIPAA" healthcare data is being addressed, and how the privacy interests of individuals are being protected (if at all) for this non-HIPAA healthcare 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 web sites gather and distribute healthcare information without the involvement of a covered entity (meaning that these web sites are not covered by the HIPAA Rules). These range from commercial health information web sites, to patient support groups, to personal health records. There has been a significant expansion of mobile applications directed to healthcare data or offered in connection with health information or overall wellness. The entire concept of wearables post-dates the

HIPAA Rules and generally such wearables fall outside the scope of the HIPAA Rules. The growing expansion of "direct to consumer" healthcare activities primarily avoid regulation by the HIPAA Rules. A wide range of the largest tech companies in the world also are becoming involved — to varying degrees and through varying means — in the collection and analysis of health-related data. Unless a HIPAA covered entity is involved, these activities generally are outside of the scope of the HIPAA Rules, and are 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 and have reasonable and appropriate security practices).[6]

In addition, as "patient engagement" becomes an important theme of healthcare 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.[7] The complexity of the regulatory structure (where protections depend on sources of data rather than "kind" of data), and the 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 healthcare data overall. There are meaningful situations across the healthcare spectrum that involve data that is 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 re-evaluation of the overall HIPAA framework.

At the same time, there also has been an increased usage by HIPAA covered entities of personal data that would not traditionally be viewed as "healthcare information." As just one example, the New York Times reported on "health plan prediction models" that use consumer data obtained from data brokers, such as income, marital status, and number of cars owned, to predict emergency room use and urgent care needs.[8] A 2013 study by the SAS Institute[9] found that television usage patterns, mail order buying habits and investments in stocks and bonds were all variables with predictive power to understand patient risks for particular health outcomes. This kind of information usage by HIPAA covered entities — relying on data that is not traditionally viewed as healthcare information and which is widely available outside of healthcare contexts and for a wide variety of non-healthcare usages — threatens to blow up the concept of what "health information" means.

This convergence of data creation and usage is leading to an increasing debate about what should be done, if anything, about this non-HIPAA healthcare data and the application of the HIPAA Privacy Rule to data that does not directly involve the provision of healthcare. It is clear that this debate will be ongoing and extensive. It is not clear at all what the results of the debate will be.

Today's Discussion

Moving to the current debate about a national privacy law. Driven by the GDPR, the CCPA, and a broad variety of privacy and data security "scandals" involving tech companies, large scale security breaches and the like, there has been a

more extensive debate about a national privacy law than at any point in American history. How can the approach taken for healthcare data help guide this discussion?

What can be Learned from the HIPAA Model?

For better or worse, the core elements of the HIPAA Rules can be summarized as follows. The HIPAA Rules incorporate 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 U.S. approach to privacy law, which is one that has favored sector-specific regulation. It then incorporates a means of addressing service providers (first by contract, then by law after legislative change).[10]

One of the key choices in the development of the HIPAA Privacy Rule — one that can be an enormously useful model in the development of a national privacy law — involves the approach to consumer consent and the related ability of these covered entities to use and disclose regulated information. The idea of "consent" under the HIPAA Privacy Rule is straightforward – consent is presumed for certain key areas for uses and disclosures of personal information, tied to "normal" operations of the healthcare industry. For this set of purposes — Treatment, Payment and Health Care Operations — consent is presumed under the law.[11] (Note that, unlike some other laws such as the Gramm-Leach-Bliley Act,[12] which focuses its privacy obligations on disclosures of personal information, the HIPAA Privacy Rule applies to both uses and disclosures of information). This defined set of "permitted" purposes is tied both to normal activities that we want to encourage in the healthcare system (for the benefit of all healthcare stakeholders) and to effective operations of the healthcare system, consistent with consumer expectations. Note that this idea of "appropriate" purposes for permitted disclosures seems consistent with the idea of "context," which has emerged in the Obama Administration Consumer Privacy Bill of Rights[13] and other emerging views on a future privacy law.

The HIPAA Privacy Rule also permits disclosures for certain public policy purposes under section 512 of the HIPAA Privacy Rule, such as 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.[14]

The HIPAA Privacy Rule incorporates 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. The HIPAA Rules also include a separate set of security principles and a 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.

Other Healthcare Privacy Regimes

How else can the privacy of healthcare information be addressed? Remember, HIPAA is not really a health information privacy rule — it is a rule that protects certain information in certain contexts when held by certain kinds of entities. Other regimes have chosen different approaches to healthcare privacy.

GDPR

GDPR takes a very different approach from HIPAA. Under GDPR, health information is treated as sensitive data, but there are no specific requirements for the healthcare industry per se. 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 United States 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 GDPR). There is very little additional consideration in GDPR of the healthcare industry on its own.

The California 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 (CMIA).[15] This is a freestanding law different from CCPA (described below) 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. It is extremely challenging — to say the least — to evaluate the differences between the HIPAA Rules and the CMIA for HIPAA covered entities (and very difficult to apply the law to other kinds of entities that appear to be subject to it), as the CMIA incorporates some portions of the HIPAA Rules, adds other items, subtracts some, and writes others in different ways using similar but not identical words for similar practices. The approach of this law is to define the healthcare industry in its own way, and then to impose a similar set of use and disclosure limitations on that industry. The defined industry not only includes the healthcare providers and health plans subject to HIPAA, but also includes:

Any business that offers software or hardware to consumers, including a mobile application or other related device that is designed to maintain medical information, in order to make the information available to an individual or a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis, treatment, or management of a medical condition of the individual, shall be deemed to be a provider of health care subject to the requirements of this part. California Code, Civil Code - CIV § 56.06(b).

There is a somewhat analogous law in Texas[16] (analogous both as to the CMIA's broader scope and its overall ambiguity about who it applies to and confusion about how it is similar to or different from the HIPAA Rules).

CCPA

Then, since California is not confusing enough for healthcare, we now superimpose CCPA on the existing structure. CCPA is a general, all-purpose privacy law generally applicable to all personal information of California residents. 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 (so an accounting firm that provides services to hospitals is exempted for that work, but not for its work involving banks or retailers). Intriguingly, it also exempts entities covered by the CMIA. 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 healthcare information in some way (with the potential exception of certain employer-collected health information not subject to HIPAA). CCPA, however, is emphasizing the challenges for an industry that now regularly crosses the lines for these different laws because of the business and compliance challenges of applying different standards to the same or similar business practices, depending on details about particular business relationships or data flows.

Federal Concepts So Far

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

The Klobuchar/Murkowski Proposal[17] 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 legislative history. While recognizing the problem, it takes a "first step" approach to a solution: it requires a task force and then regulations "to help strengthen privacy and security protections for consumers' personal health data … collected … by consumer devices."[18] It provides a specific set of topics for regulators to consider under the legislation. This proposal targets this current gap, but would not create a uniform set of rules across the industry, as there would still be different rules for data covered by the HIPAA Rules compared to non-HIPAA data.

Other approaches are more general, and take varying approaches to how a new law would intersect with HIPAA. The Wyden bill[19] is mainly focused on expanding and increasing Federal Trade Commission (FTC) authority. This bill

would presumably allow the FTC to treat non-HIPAA companies the same as other companies under their existing standards, and does not challenge the FTC's authority in connection with HIPAA covered entities.

The Intel proposal — a carefully thought-through private sector initiative — primarily focuses on modified and expanded FTC authority as part of its broad overall approach to privacy regulation.[20] It includes some specific requirements related to health information. It provides certain preemption, but not for laws that go beyond HIPAA. It excludes HIPAA covered entities generally.

Another approach from Senator Schatz[21] defines "sensitive data" to include healthcare data. Again, its focus seems to be on the FTC. However, unlike other proposals, the obligations seem to be superimposed on HIPAA.

Senator Rubio's proposal[22] includes medical history and biometrics as categories of data subject to the law but not health data overall. It generally exempts entities subject to HIPAA and preempts state law.

The broader Senator Markey privacy proposal[23] includes health information among the protected data elements. While the language is somewhat unclear, it seems to apply in addition to HIPAA.

In the House, Congresswoman DelBene has introduced "The Information Transparency & Personal Data Control Act."[24] This proposal creates a wide range of obligations related to "sensitive personal information," including health information, but does not otherwise address the healthcare 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?

There will be significant debate over the next few years on the future of a federal privacy law. While it might be possible for a healthcare "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 healthcare data (with an obvious ambiguity about what "healthcare data" would mean);

- A set of principles (through an amendment to the scope of HIPAA or some new law) that would apply to all healthcare data; or
- 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 "healthcare information."

In parallel consideration, a national privacy law could:

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

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

Conclusion

Despite the importance of the healthcare industry, the HIPAA Rules, and health information to the overall debate about individual privacy, healthcare has not been a leading factor in the current national privacy legislative debate. This is unfortunate and can lead to problems for both the healthcare industry and a variety of other stakeholders interested in healthcare data and the privacy of this data. The HIPAA rules — because of their detail and our broad experience with them since their implementation — can provide some useful experience in evaluating the national debate, particularly in the HIPAA Privacy Rule's approach to consent and the use and disclosure of covered information.

In general, the healthcare industry and most relevant stakeholders are comfortable with the HIPAA Rules' approach and the overall impact of the rules on the operation of the healthcare industry and the protection of patient data. Despite this comfort, the healthcare 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 healthcare industry. These differing standards create confusion and complexity that easily could be reduced through a common standard. These same challenges emerge in the discussion over preemption: if a national privacy law preempts state law,

but HIPAA covered entities are not subject to the national law, then presumably they will remain subject to state law. The healthcare industry should be evaluating whether a common standard — even if different from the HIPAA Rules — would be better for the industry and for consumers.

Today, while the healthcare industry, the patient community, and broad variety of interested stakeholders all pay close attention to these privacy programs and the overall protection of patient data, this perspective is not obviously a part of the expanding national debate. This is a mistake. Both those in Congress and the healthcare industry need to be focusing on these issues involving health information, and should be thinking about the important role of privacy protection for health information in the broader context of an appropriate national privacy law.

About the Author

Kirk J. Nahra *is a partner with WilmerHale in Washington, D.C., where he co-chairs the firm's global Cybersecurity and Privacy Practice. A graduate of Georgetown University and Harvard Law School, he teaches Information Privacy Law and Health Care Privacy Law at the Washington College of Law at American University. He also is a fellow with the Cordell Institute for Policy in Medicine & Law at Washington University. He can be reached at 202.663-6128 or kirk.nahra@wilmerhale.com.*

---

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, *available at* https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016R0679 (effective May 2018).

[2] The California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et seq. (effective January 1, 2020).

[3] Health Insurance Portability and Accountability Act of 1996, P.L.104–191.

[4] The "HIPAA Rules" mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Part 160 and Part 164. The HIPAA Privacy Rule is the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R., part 160 and part 164, subparts A and E. The HIPAA Security Rule is the HIPAA Security Standards (45 C.F.R. Parts 160 and 164, Subpart C). The HIPAA Breach Notification Rule is the Notification in the Case of Breach of Unsecured Protected Health Information, as set forth at 45 C.F.R. Part 164 Subpart D.

[5] As part of the rules implementing the provisions of the HITECH Act of 2009, which amended HIPAA, the "reach" of the HIPAA Rules was extended in part to "business associates," but this extension did not change the need to have a relevant "covered entity" involved in any collection of information.

[6] An important HHS publication tried to define the scope of regulation for this non-HIPAA health data. This report is very useful, although the relevant guidelines and provisions evolve regularly. *See* Department of Health and Human Services, "Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA," *available at* https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf.

[7] Substantial questions remain about whether patients appropriately can access their own health information. *See* McGraw, "The Patient Record Scorecard: What is it and Why we did it," (Aug. 14, 2019), *available at* https://www.ciitizen.com/the-patient-record-scorecard-what-is-it-and-why-we-did-it/.

[8] *See, e.g.*, Singer, "When a Health Plan Knows How You Shop," (*New York Times* June 28, 2014), *available at* http://www.nytimes.com/2014/06/29/technology/when-a-health-plan-knows-how-you-shop.html?_r=0.

[9] Garla et al., "What do your consumer habits say about your health risk? Using third-party data to predict individual health risk and costs," Paper 170-2013, SAS Global Forum (2013), *available at* http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.381.2705&rep=rep1&type=pdf).

[10] The original HIPAA Privacy Rule created the concept of business associates, who are service providers to covered entities. In the HITECH Act, Congress extended the scope of coverage for portions of the HIPAA Rules to apply directly to these business associates.

[11] 45 C.F.R § 164.506(a).

[12] P.L. 106–102, 113 Stat. 1338, enacted November 12, 1999.

[13] The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (February 2012), *available at* https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf (Appendix A).

[14] 45 C.F.R. § 164.502(a).

[15] CALIFORNIA CIVIL CODE §§ 56-56.16.

[16] TEXAS HEALTH & SAFETY CODE § 181.001 *et. seq* ("Texas Medical Privacy Act").

[17] S. 1842, 116th Congress, "Protecting Personal Health Data Act," *available at* https://www.congress.gov/bill/116th-congress/senate-bill/1842.

[18] S. 1842, SEC. 4(a).

[19] "Consumer Data Protection Act'' (discussion draft), *available at* https://www.wyden.senate.gov/imo/media/doc/Wyden%20Privacy%20Bill%20Discussion%20Draft%20Nov%201.pdf.

[20] Intel, "Draft Model Privacy Law," *available at* https://usprivacybill.intel.com/legislation/

[21] S.3744, "Data Care Act of 2018," *available at* https://www.congress.gov/bill/115th-congress/senate-bill/3744.

[22] S.142, "American Data Dissemination Act," *available at* https://www.congress.gov/116/bills/s142/BILLS-116s142is.pdf.

[23] S.1214, "Privacy Bill of Rights Act," *available at* https://www.congress.gov/116/bills/s1214/BILLS-116s1214is.pdf.

[24] H.R. 2013 116th Congress, *available at* https://www.congress.gov/bill/116th-congress/house-bill/2013/text.