August 17, 2020

Can HIPAA be Saved? The Continuing Relevance and Evolution of Healthcare Privacy and Security Standards

By Roy Wyman, Esq., Nelson Mullins, Nashville, TN

From the American Bar Association's The Health Lawyer

While technology has radically impacted healthcare in the United States for decades, COVID-19 is further forcing major restructuring of the healthcare system and impacting the privacy of patient information and IT security. Important changes to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations[1] are desperately needed. A review of HIPAA's history, and concerns with HIPAA's current approach, require consideration of new strategies towards privacy and security. They include:

- To the extent possible, incorporating HIPAA into broader privacy and security rules that govern *all* business entities. Broader scope also would allow eliminating vague and arbitrary distinctions between "covered entities" and "business associates."
- Addressing the unworkability of determining what information is "identifiable," and instead looking at information based on its sensitivity and criticality.
- Setting fixed, known standards for security and privacy rather than leaving information at risk under the illusion that a small entity, implementing "reasonable" standards, can sufficiently protect its data.
- Limiting rights of patients in their data (e.g., deletion and access) to large entities and those that process significant amounts of sensitive or critical information.
- Removing redundant notices that regurgitate regulatory requirements.

HIPAA in 1996 and 2000 — the Context

In 2000, Nokia released the 3390 cell phone. It could hold up to 459 characters of text and included functionality such as a phone, texting, and playing "Snake." That year Garmin had not yet released its first navigation device and the iPod did not exist.

Four years earlier, Destiny's Child and Beyoncé Knowles were about to hit it big and then-President Bill Clinton signed HIPAA. The law was then viewed as a sea change: in the portability of insurance. Careful observers noted that it also included some revisions to how healthcare services would be billed. The law was not immediately recognized as a major privacy and security bulkhead, primarily because it contained no privacy or security standards. Rather, Congress promised that it would return to the issues of health information security and privacy. It did so by ordering the Secretary of Health and Human Services (HHS) to submit recommendations on a privacy and security law within 12 months. If, after that, Congress still had not passed a law, the Secretary was to develop and implement regulations covering these issues.

When Congress failed to act, the Secretary did, but in a very different context from today. In 1996, many healthcare providers continued to use paper records and file paper claims.[2] In fact, many providers—physicians in particular—were slow to adopt any sort of electronic records.[3] Filing paper claims was inefficient and expensive, and promoting electronic filing was a clear

goal of the HIPAA legislation. In addition, various health insurance plans required different forms and codes regardless of how those forms were filed. At the time that HIPAA regulations were promulgated, HHS estimated that 400 different formats for Electronic Data Interchanges were in use.[4] By promulgating a single form and set of codes, and requiring that payors accept all claims submitted in that form, a great (but under-reported) success of HIPAA has been the increase in electronic filing, simplification of filing rules, and reduction in costs related to billing.[5]

A natural concern arose that the now-promoted electronic transmissions could be intercepted or otherwise used improperly. For example, a criminal might be able to intercept electronic payments from a payor to a provider or sensitive health information intended for the payor.[6] The HIPAA Security Rule [7] provided the first set of standard measures in the healthcare industry specifically addressing the confidentiality, integrity and availability of health information.[8]

A common perception is that prior to HIPAA, privacy was not as significant of a concern as it is today and the privacy provisions of HIPAA were an afterthought.[9] While privacy concerns are almost certainly more "front-of-mind" for individuals today, a look at polling suggests that public support for privacy rights has been strong and consistent since the mid-90's. For example, a *Money Magazine* poll in August 1997 found that 74 percent of the public were "somewhat" or "very concerned" about threats to privacy, and 88 percent of the public favored a privacy "Bill of Rights" that would require businesses to disclose the types of personal information collected and how it would be used.[10] By *non*-contrast, a poll in December, 2019 by Morning Consult of registered voters found that 79 percent of Americans believe that Congress should enact privacy legislation and 65 percent of voters said data privacy is "one of the biggest issues our society faces."[11]

How HIPAA addressed Privacy and Security

In addressing HIPAA's relevance and future, it is useful to consider its approach, which was part of what is described here as the "First Wave" of privacy and security rules. This wave included HIPAA and the Gramm-Leach-Bliley Act (GLBA),[12] and these laws and/or regulatory schemes[13] are marked by a few, common elements (referenced here as "badges")[14]:

1) Each addresses a specific industry, activity or concern rather than regulating universal activities (e.g., "covered entities" under HIPAA).
2) The restrictions addressed one type of information (e.g., health ("protected health information" or "PHI") or financial information).
3) An attempt is made to keep rules "flexible" such that larger entities would be held to a higher standard than smaller entities or those with simpler activities.

   a. Consistent with a "flexible" approach, IT security regulations avoided specific requirements, emphasizing creation of a *process*.[15] Broadly speaking, that process involved at least three elements: a risk assessment; an on-going and evolving risk management plan; and "administrative" safeguards such as naming a security officer and executing agreements with vendors.

   b. Where standards were required, the regulators demurred from creating them and looked to existing, independent standards bodies, with adherence often voluntary but with benefits for compliance. For example, the HIPAA Security Rule does not strictly require encryption. It does, however, say that encryption in compliance with standards published by the National Institute of Standards and Technology (NIST) will be considered "secured."[16]

4) Each creates individual rights, for example, for access, amendment of incorrect records, to know of any breaches and accounting of how records were used.
5) Reliance on public disclosure: entities are required to post and provide a Notice of Privacy Practices or a Privacy Policy so

that individuals understand their rights and how information is used.

6) No private right of action is created. While individuals may file complaints, only a governmental agency can bring suit or levy a fine for violations.

One element that is omitted from these statutes is a mandatory consent requirement.[17] As such, covered entities may use sensitive information for permitted purposes without the consent of an individual.

Why are these Concepts Not Working?

It is important to acknowledge that HIPAA is still the law of the land and it has largely worked. Twenty-five years ago, health information was often unprotected except to the extent that paper records created "security by obscurity." Records were largely kept private primarily because of ethical standards and individuals' personal integrity.

Notwithstanding that success, HIPAA has proven to be imperfect from its conception, and it does not always age well, particularly because the world has changed radically on two fronts: the technological and the cultural. On both fronts, the six badges have revealed structural weaknesses.

The Structural Issues

Business Associates

The first regulatory badge was a limitation of statutes to a particular industry. In the case of HIPAA, the statute was limited to "covered entities," which are defined as healthcare providers, plans and clearinghouses.[18] Immediately, the regulators drafting regulations had a problem — HHS only had jurisdiction over "covered entities." Yet many entities didn't qualify as covered entities but received PHI. HHS could not directly regulate collection agencies, billing companies, record management companies and numerous others that receive PHI.[19] To address this flow of PHI, HHS created the concept of a "business associate," which included any entity that collects, accesses or uses PHI on behalf of a covered entity. It then created an exception to the HIPAA Privacy Rule to permit utilization of business associates so long as the covered entity entered into a "business associate agreement" with each business associate. Though HHS, at the time,[20] could not directly regulate business associates, it *could* go after the covered entity. HHS thus deputized each covered entity, forcing it to police its vendors.

While Congress attempted to address this oversight in the HITECH Act of 2009, which amended HIPAA, it did so by adopting the regulations' definition of a "business associate." Thus, if a company receives health information *on behalf of* a covered entity, it is subject to HIPAA. If that same company receives health information directly from, and on behalf of a person or entity that is not subject to HIPAA, such as an individual, it is *not* covered by HIPAA. Entities that are not covered entities or business associates can gather, disclose and sell health information without oversight from HIPAA.[21] This historical oddity means that two companies holding the same information are treated differently depending on contractual relationships.

Scalability

The HIPAA Security Rule promised that its requirements were "scalable,"[22] that is, that smaller entities would have lower compliance standards than larger entities. In reviewing scalability, consider two types of costs — direct and secondary. Direct costs include fees for virus software, firewalls, etc. Such costs under the HIPAA Security Rule are scalable to the extent that smaller entities will implement fewer protections or protect fewer assets. A major burden of the HIPAA Security Rule, however, is its complexity, which can impact all covered entities more equally.[23] The HIPAA Security Rule includes 42 specifications (each either "required" or "addressable") divided into 18 standards and three broad categories. A common perception is that

covered entities must adopt all "required" specifications and may freely ignore "addressable" specifications. Before considering specifications, the HIPAA Security Rule first requires that entities ensure the confidentiality, integrity and availability of PHI and protect against any reasonably anticipated threats. If an entity adopts only required specifications, but hasn't protected against relevant threats, the entity is not in compliance with the HIPAA Security Rule.[24] Further, if a specification is listed as "addressable," the entity *must* assess whether the specification is a reasonable and appropriate safeguard and either implement the specification or document why it would not be reasonable and often must implement an equivalent alternative measure.

A real-world example illustrates some HIPAA Security Rule shortcomings. Under the section "Administrative Safeguards,"[25] the HIPAA Security Rule mandates adoption of the "security awareness and training" standard. Within that standard are the "Log-in monitoring" and the "Password management" specifications. No explanation is given for why such elements are considered part of "security awareness and training," as these are most often automated processes. Nor is there an explanation how these standards intersect with "Access control" requirements, which are addressed under both the "technical safeguards"[26] and "physical safeguards"[27] sections. Log-in monitoring is "addressable," and HIPAA allows that an entity might not implement the standard. One wonders what would be an alternative, reasonable approach? Perhaps a pad of paper and pen next to each computer with each employee writing down the time of logging in and out and listing each file accessed? This level of "scalability" has at least two significant weaknesses: (1) it is a trap, luring entities into adopting inexpensive but risky approaches to security that do not meet the requirements of the HIPAA Security Rule; and (2) the secondary costs of understanding all of the requirements, and documenting and implementing reasonable solutions, are significant. One might argue that a mandated solution (e.g., for electronic monitoring of access to systems), while increasing direct costs for some entities, would more than offset those costs by reducing secondary costs of consultants, documentation and training.

These secondary costs have forced healthcare entities to take one of two approaches — either spending large amounts on consultants and legal counsel or taking a "Do-it-Yourself" approach involving slap-dash assessments, pulling documents from the internet, and assuming huge risks.[28] To the extent that assessments, policies, and other documents are not specific to the entity, or apply to a different entity and therefore are not followed, they do not comply with HIPAA.[29]

Transparency — Notification

An additional badge of First Wave rules was a philosophy that favored transparency by requiring publication of privacy policies. In practice, these notices have not proven to be effective: nearly all HIPAA-required Notices of Privacy Practices (NPPs), for example, are substantively identical, parrot the requirements of the regulations, and are generally ignored. By way of evidence, NPPs provide information regarding a number of individuals' rights, yet the utilization of these rights appears to be very low.[30]

The Technological Issues

If today's technology was identical to the technology in 2000, the above issues alone would undermine HIPAA. Drastic changes in technology further threaten the edifice of healthcare privacy and security. Look first at historical changes and then at currently developing technologies that undermine HIPAA.

Identifiers and Covered Information

The HIPAA regulations contain a broad definition of "individually identifiable health information," including information that identifies an individual or "with respect to which there is a reasonable basis to believe the information can be used to identify the individual." When such identifiers are combined with health-related information, they become PHI.[31]

Based on this definition, if one removes from PHI either all health information or all identifiers, it no longer meets the definition of PHI and is not subject to HIPAA.[32] The HIPAA regulations provide two methods for "de-identifying" information such that it is no longer PHI (with the corollary that if information meets one of such methods, it was never PHI).[33] Under either standard, there must be "no reasonable basis to believe that the information can be used to identify an individual." The most common method for de-identification, known as the "safe harbor" method,[34] requires removal of 18 identifiers including such anticipated items as names, account numbers, and addresses, as well as some that are more surprising, such as more than the first three digits of a zip code and any element of a date other than year.

In the face of advancing technology, the safe harbor method has proven both over-inclusive and under-inclusive. For example, many entities will use data that includes a date of service. If analyzing millions of records for services throughout the United States, with the only "identifiable" information a single date of service, absent unusual circumstances there appears little risk that the information will identify an individual. On the other hand, artificial intelligence and other technologies addressed below make it more likely each day that information with none of the 18 identifiers can be used to identify an individual.

Cloud Providers — Poster Children for Over- and Under- Inclusion

Today, the idea of "cloud computing" seems commonplace and ubiquitous. The concept did not become common until 2006, however, when Google, Amazon and others began using the term to describe accessing software and files on the Web rather than on a desktop. For a decade no one was sure of the extent to which HIPAA governed PHI stored in the cloud. Cloud providers argued that they often were not business associates because in many cases a covered entity or business associate stored only encrypted PHI in the cloud, and the provider by contract could not access, use or disclose the PHI. In 2016, HHS finally settled the matter by determining that cloud providers were business associates, even if just storing PHI.[35] Although cloud providers may complain that they should not be subject to HIPAA absent access to PHI, and it is easy to read this as HHS simply applying a literal reading of the regulations that cover "maintenance" of PHI, beneath the surface are two tensions. First is the weight to be given to the availability of PHI and threats to it. Second is the seemingly capricious nature of HIPAA's definitions where a business can house the exact same information yet be subject to different laws based on internal workings of its customers. These tensions begin with the concept of "availability."

Availability — Ransomware and Blockades

An issue not as widely discussed in 2000, but very relevant today, is the availability of PHI. This issue has been addressed in two contexts by HHS, as it has been forced to deal, sometimes inconsistently, with the issue. While one can argue that HHS' views regarding cloud providers arose from a literal reading of HIPAA rules, HHS did not take a literal approach when addressing the issue of ransomware — malware that encrypts data on a victim's system so that the victim cannot access it.[36] By a literal reading of HIPAA's regulations, if a ransomware attacker does no more than encrypt a system via ransomware, it actually makes the data "secured ePHI." By this view, introduction of ransomware would *not* appear to create a breach under HIPAA's Breach Notification Rule.[37] HHS in January 2018 addressed the issue in a Fact Sheet[38] and stated, "When electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI...was acquired (i.e., unauthorized individuals have taken possession or control of the information)...." While the above language is arguably a stretch based on the Breach Notification Rule, it would seem dispositive on the question. The Fact Sheet goes on to state, however, that, "Unless the covered entity or business associate can demonstrate that there is a '...low probability that the PHI has been compromised,'...a breach of PHI is *presumed* to have occurred."[39] Whatever its shortcomings, the Fact Sheet reveals a concern within HHS regarding the availability of PHI. Where access is blocked, a HIPAA breach may be triggered.

Likewise, HHS has taken up the issue of PHI-blocking by business associates. For example, certain cloud providers, claiming that a covered entity owes it money, have refused to allow access to PHI until all amounts are paid. In response, HHS published an FAQ[40] stating that a business associate may not block access by a covered entity to PHI maintained by the business associate, including for failure to pay all fees due. While one may understand the concern when a cloud provider reduces the availability of health information in order to extract payment, no similar concern is applied where the information is equally sensitive but not health related.[41]

The rise of ransomware, cloud providers and data blocking were not envisioned in 2000 and underscore the need for updated regulations addressing new risks.

New Methods of Computing

Of the many changes in technology whose full impact could not be seen when HIPAA regulations were released, among the most significant are those that are likely to have the largest impact over the next decade including distributed ledger technology (DLT or "Blockchain"), quantum computing and artificial intelligence (AI)/machine learning. While the impact of each of these technologies on healthcare privacy and security is worthy of its own article,[42] this article touches on each briefly.

Distributed Ledgers

Blockchain is best known for being the technology underlying Bitcoin. At its heart, most Blockchains can be thought of as layering three levels of technology.

At the bottom is a network of connected computers acting as witnesses to any transaction that occurs. This network is a critical part of documenting and approving transactions. For example, if Jane, a member of a network, wishes to transfer one Bitcoin to John, at least 50 percent of all of the members of the Bitcoin network plus one must agree that Jane owns that coin. The advantage of the network is two-fold. First, any "hack" of the network would require hacking more than 50 percent of all of the members of the network. Second, neither Jane nor John needs to go to a central bank or other authority. As such, there is no need to trust any central regulator. The network regulates itself.[43]

The middle layer is the protocol software that enables and provides utility to the network. In other words, it creates, in code, the rules connecting and allowing the network and its ledger.

The top layer is the operative software. For example, this is the "Bitcoin" layer that is the digital currency. This layer, however, can be used for many use cases such as just-in-time supplies, instantaneous filing of claims and payments and inventory control assuring that drugs and supplies are not counterfeit. While the potential for Blockchain to solve many issues facing healthcare is enormous, none of this was a consideration at the time of HIPAA regulations. While many legislative attempts to address Blockchain have failed to promote the technology and have unwittingly made its implementation more difficult,[44] HIPAA currently does not preclude most use cases for Blockchain (including the long-sought "holy grail" of accessing electronic health records (EHRs)).[45] Ironically, however, changes in the law could severely limit use of Blockchain. For example, the European Union General Data Protection Regulations (GDPR) [46] and the California Consumer Privacy Act (CCPA) ,[47] both of which are discussed more fully below, make certain Blockchain use cases difficult or impossible.[48] While there is no evidence that such limitations were intentional, the laws were drafted in a manner that was insensitive to the technology. There is a danger that revisions to privacy laws, including HIPAA, could similarly endanger Blockchain.

Quantum Computing -- Encryption

To explain quantum computing requires entering a strange world where, for example, electrons can be in multiple places at once while spinning up, down or "not yet determined," and particles that are light years apart in completely different eras can nonetheless affect each other. Further, the impact of quantum computing may not be known for decades. This article therefore will focus on just one aspect of the technology: encryption. Traditional encryption involves using a "key" to scramble information on one's computer, which information can be unscrambled by that same key. That "key" is a set of digits sufficiently long that a traditional computer could not, in a reasonable amount of time using reasonable resources, determine what it is. The goal for quantum computers is to be a completely unreasonable computer that can do exactly those sorts of calculations in a ridiculously small amount of time.

The upside to quantum processes is that they hold the potential to make messages and data basically unhackable.[49] The downside is that for any parties not utilizing quantum encryption, current methods would be largely futile to stop quantum hacks. According to a report by the RAND Corporation,[50] such quantum code-breaking could occur in 12 to 15 years. NIST has been reviewing quantum-resistant cryptography, but there is no obvious approach for entities that will not have the wherewithal to adopt quantum solutions. In reviewing how security requirements might adapt to quantum technology, they could, first, mandate encryption and, second, mandate that companies adopt whatever standards NIST or another standards-setting body may propose in the future. In turn, that potential solution reveals a deeper, two-fold structural concern with HIPAA. First, this would undercut the "scalability" model by imposing a very specific, and very high, standard. Second, it underscores the reality within security that there are haves and have-nots. Have-nots, such as small providers, are unable to protect themselves against malicious attacks from haves such as state actors and hacktivist conglomerates.

Artificial Intelligence and Machine Learning

In several regards, HIPAA is built on an assumption that information can be categorized as identifiable or not identifiable; health-related or not health-related. In 2000, one could make a case that it is known whether there is a reasonable basis to believe that information can be used to identify an individual.[51] Machine learning and the broader enterprise of AI, however, are expert at finding patterns to identify individuals using minimal information.

For example, more than 10 years ago as part of a competition, Netflix released anonymized information including the age, gender, zip code, genre ratings, and previously chosen movies for a large data set. Unexpected to Netflix, security experts showed that such "de-identified" information could be used to identify individuals.[52] Studies have shown that de-identified patient information can be re-identified,[53] and the growing power of AI has made it easier to identify more patients using less data. As noted above, the most common method for de-identifying information under HIPAA utilizes a very imprecise measure that often can be, by turns, overly restrictive or not restrictive enough. That method does not fully take into account the relative sophistication and intent of parties receiving de-identified information. While most individuals could not re-identify data based on an IP address and browser history, several companies earn a good amount of money doing exactly that. Beyond just re-identifying data, AI has the potential to help track, identify and create profiles of individuals.

While perhaps the stuff of sci-fi, AI also can be seen as an independent intelligence that no individual is fully responsible for. For example, in July 2019 two patent applications were filed for inventions created by AI.[54] In a situation where AI, on an open network not owned by a specific entity, accesses or re-identifies PHI, how does HIPAA or any other law identify the relevant "covered entity" or other actor?

Where do We Go from Here?

The Second Wave

While HIPAA, even with its HITECH upgrade, has mostly been locked in amber since 2009[55] (and arguably since 2000), a new, "Second Wave" of privacy and security regulations has swept in, highlighted primarily by GDPR but also including regulations in a number of other countries as well as CCPA and, to a lesser degree, the New York Stop Hacks and Improve Electronic Data Security Act (SHIELD Act).[56] While GDPR contains provisions that would sound familiar to HIPAA aficionados, the basic structure of Second Wave statutes is fundamentally different. As noted above, the First Wave of regulations was marked by several "badges" including:

1. Addressing only one industry,
2. Restricting specific types of information,
3. Prioritizing "flexible" approaches,
4. Creating individual rights,
5. Requiring public disclosure, and
6. Removing private rights of action.

With the Second Wave, only badges 4 and 5 truly survive, though they flourish.

Second Wave rules create a structure of data "controllers" and "processors" ("businesses" and "service providers" under CCPA). While this may sound similar to "covered entities" and "business associates" under HIPAA, the distinctions are important. First, unlike First Wave statutes, GDPR and CCPA are not limited to a particular industry. Further, a "controller" is not defined by whether it collects "personal data," but rather by whether it "determines the purposes and means of the processing of personal data".[57]

From this subtle distinction flows numerous consequences. First, there is the potential for "joint controllers," as more than one entity may control the means of processing data. Second, processors may only process personal data on "documented instructions from the controller." The control exercised by a controller is far higher than under HIPAA (e.g., each sub-processor must be approved by the controller). The third implication is a bit more philosophical but no less impactful — the controller must take a much more active role in protecting personal data *from the perspective of the data subject*. For example, under HIPAA, so long as a use or disclosure of information meets an exception, it is permitted. Under GDPR, however, the controller must process data for a specific, explicit and legitimate purpose and the processing must be lawful based on a handful of reasons such as consent or necessity (e.g., performance of a contract). If based on consent, it must be freely given, informed and shown by "a clear affirmative action".[58] For example, in much of the European Union, it is questionable whether an employee may ever give consent, as the power difference between the employee and employer indicates that consent may never be "freely given." Where a type of processing raises a high risk to the rights and freedoms of natural persons, the controller must carry out a "data protection impact assessment" weighing the impact of the processing of personal data.

These requirements do not reveal the "scalability" sought under HIPAA — they are fixed for all entities, regardless of size, doing business in the European Economic Area.[59]

By contrast, badges 4 and 5 of the First Wave appear again in the Second Wave, but with much greater force. For example, in addition to rights to amend and receive access to personal data, GDPR and CCPA also provide a "right to be forgotten"(i.e., deletion) and a right to opt-out of sales of information; GDPR also includes a right to object to certain uses of data, to opt out of marketing and to not be subject to decisions based on automated processing. Notice requirements also are made much more burdensome on entities. For example, under CCPA, a business may need to provide a consumer, at various times, with four different notices: a Privacy Policy, Notice at Collection, Notice of Right to Opt-Out and Notice of Financial Incentive.[60]

Finally, unlike badge 6, Second Wave rules sometimes include private rights of action in the event of a breach. GDPR very

much includes such a right, while CCPA permits certain claims for violation of security provisions.

Current Federal Bills and Fixing the Current Rules

Facing the limitations of First Wave laws, particularly their limited scope, some U.S. states have introduced, and California has passed, general privacy bills. Rather than simplifying the current network of complex and conflicting laws, these bills threaten to create an additional patchwork of inconsistent requirements such that a company doing business across the country could be hampered in attempting to apply a single compliance program. For this reason, with the prompting of privacy and security rights groups as well as some larger corporations, Congress has introduced or discussed several bills attempting to address privacy and security.[61] While they have significant differences, they all share similarities and many elements of the Second Wave statutes.

While each of these bills will be subject to revision, in reviewing their tone and approach, consider whether they address the weaknesses identified above within HIPAA. If not, stakeholders may need to consider alternative approaches.

1) Jurisdiction—Who's Covered?

The first badge of First Wave rules was their limitation in scope — only certain industries were covered. The proposed federal bills offer a broader approach but still with limits that could create arbitrary distinctions. For example, S.2986, the Consumer Online Privacy Rights Act (COPRA) and S.3456, Consumer Data Privacy and Security Act of 2020 (CDPSA) would cover, for the most part, any entity that is subject to the Federal Trade Commission Act[62] (generally, any entity other than financial institutions, common carriers, air carriers and those subject to the Packers and Stockyards Act), and neither would preempt HIPAA or GLBA.[63] As such, these bills would leave HIPAA in place, but could cover personal information held by a HIPAA-covered entity that is not health information. This would leave two tiers of "covered entities" with very different requirements under both privacy and security. For example, security requirements for "covered entities" under these bills is likely to be less clear than under HIPAA. Allowing HIPAA (and GLBA) to exist alongside a broader privacy bill neither resolves current issues with HIPAA nor creates a single set of rules for all entities to meet.

This bifurcated regulatory scheme does not address the situation of vendors working across industries such as those poor[64] cloud providers described above who do not access PHI yet are business associates under HIPAA. Which entities qualify as business associates is the result of an historical oddity, and the proposed regulations do not address the situation where two companies with exactly the same information may be treated differently depending, for example, on whether it contracts with an individual consumer or a physician. Second Wave rules do not address this concern but rather enshrine it in the distinction between "controllers" and "processors."[65]

An alternative: In contrast to Second Wave approaches, one might recommend that any re-writing of HIPAA or other rules cover all business entities and ignore relationships among them (e.g., who is controlling the data or on whose behalf the entity is acting). A focus on the types of information held or accessed and how it is used and disclosed could give greater clarity, simplify drafting and reduce secondary costs relating to mandatory contracting between entities.

2) Identifying the Identifiable

The second "badge" was that covered data is limited to identifiable information of a particular type (e.g., identifiable health information). This approach tends to put unwarranted faith in understanding what information is "identifiable" while drawing arbitrary lines between what is protected because of its category and not protected, though sensitive. Most of the proposed bills take the approach of GDPR and CCPA by protecting information that identifies, or is linkable to, an individual.[66] Any

information that can be used on its own or in combination with other information to identify the individual is "linkable." This definition is of little use today and likely of less use tomorrow. As noted above, in the "right" hands, information without obvious identifiers may still identify an individual: if not now — one day soon. Much information that is linkable to an individual, in the typical company's hands, cannot be used to identify anyone, and very few may know when the day has come that certain pieces of information are sufficient to identify a person. Definitions for protected information in the proposed bills remain vague, as what information is covered can shift by the day, depending on the ability of various technologies to identify individuals using less information.

An alternative: Any attempt to regulate data based on whether it contains certain "identifiers" is a fool's errand. Therefore, the best approach may be counter-intuitive — to give no firm definition of personal data or "de-identification" based on the information itself. (A definition of "identifiable" PHI could be retained as a type of "anti-safe harbor" — information that is automatically considered identifiable). If all entities are covered by a single statute, information could be limited based on its use rather than its nature (for example, limitations on robocalling do not depend on defining "identifiable" information). If Company A discloses information to Company B, and that information is identifiable to Company B, the best approach may not be to limit the sharing of information but the use of information by Company B.[67]

3) Scaling Scalability

The third badge involves security requirements that promise to be flexible and scalable, but that nonetheless create uncertainty and expense. The proposed federal privacy bills as currently drafted do relatively little to address IT security.[68] To the extent that they address security, they are in line with GDPR, which requires "reasonable administrative, technical, and physical safeguards,"[69] or similar language, that should take into account the size, complexity and resources of the entity and other variables. The concern, however, is that sophisticated actors will continue to prey upon smaller entities for whom "reasonable" security will be completely insufficient to protect sensitive information. "Scalable" approaches do not work today and will be a recipe for security disasters moving forward.

Two alternatives: Though the thought is deeply uncomfortable, the current model simply cannot address current and future security risks. Sadly, alternative options could require radical shifts in how security is viewed and handled. Here are two such options:

i. In the face of computers that are growing in power daily, the promise of quantum cryptography, and a growing gap between haves and have nots in IT security, society and legislatures may acknowledge that IT security is largely an illusion and the HIPAA Security Rule emperor has no clothes. Under this approach, the government would stop attempting to protect all identifiable data, and data that is too voluminous or common to protect simply will not be protected. For data that is truly sensitive or critical (e.g., critical to national security or the release of which could cause death, physical injury or widespread harm), the government would undertake to provide sufficient security by hosting the data itself and limiting access, and would also provide minimum standards and certifications for individuals and companies that chose to host the data themselves.

ii. A second option would be for regulators to set bare minimum standards to protect data and require that all entities holding data on behalf of others, or for business purposes, meet that level. For smaller entities that hold sensitive information or information that is critical for the broader community, the government would either subsidize their security efforts or force them to combine with other entities for their common support.

Neither of the above proposals is likely to be popular, particularly within certain sectors. Depending on one's views, they may be considered either leftist or reactionary. Of course, alternatives would be greatly welcomed, but are currently lacking. The

only thing known with certainty is that the current approaches do not work and will continue to fail in greater measure.

4) The Right Rights

Each of the significant proposed privacy and security bills in Congress includes certain rights of individuals: to know, to access, to receive in an electronic format (portability), to correct and to delete. Provision of such rights can serve an important basis for understanding how businesses use and disclose information. As noted above, these rights are exercised by an exceedingly small percentage of individuals yet create significant burdens for businesses. In short, regulation of privacy and security is not free — to the companies, governments or taxpayers. For example, the state of California estimates that implementation of CCPA will lead to a loss of 9,776 jobs and cost the state between $467 million and $16.454 billion, with net in-state investments lowered between $40 million and $1.14 billion by 2030.[70] A survey conducted by TrustArc found that 29 percent of businesses expected to spend less than $100,000 on CCPA compliance (including those who anticipated no costs), while nearly 40 percent expected to spend at least $500,000, with four percent anticipating costs of over $5 million.[71] A large part of such costs relate to mapping where particular data is housed such that, upon receipt of an individual's data request, a company may locate the relevant information, determine whether it is appropriate to delete, copy or amend, and then carry out such action, while keeping a record of such activity. While all of the privacy bill proposals provide for such consumer rights, there is little discussion of whether the benefits of those rights offset the burdens on businesses.

Regardless of whether Second Wave and proposed rules are overly burdensome, the reason that many individuals want such rights[72] is because data *has* been abused. Much of the impetus for those rules are the activities of alleged and proven bad actors who are willing to sell or use personal data for detrimental ends. If a local restaurant wants to ask for a customer's email address to send brunch offers, should it be forced to spend tens of thousands of dollars on IT security and legal professionals?

An alternative: A bifurcated approach seems preferable. First, all businesses would be required to meet minimum requirements such as opt-in or opt-out for sales of information, and certain uses would be illegal (e.g., using data to impersonate an individual without consent). Second, businesses with revenues above a certain amount, or with a certain volume of sensitive information, would be required to provide individuals with all of the rights typically described in Second Wave regulations. Such businesses are better able to build in costs in their pricing structures and, because they are most able to create societal harm, they should shoulder a higher burden of transparency.

5) Transparency and Notices

Many legislators throughout the world possess faith in the power of information to cause people to make wiser choices.[73] This faith extends to a belief that providing individuals with notices will impact whether they provide a company with information or take advantage of the rights discussed in (4) above. The approach, often falling under the rubric of "Fair Information Practices" (FIPs), has yet to show significant impact in how individuals act. The attempt to provide such notices may itself create problems such as providing individuals so many notices that they stop reading any of them.[74]

An alternative: In considering requirements for "transparency" and notice, one may well remember the State Motto of North Carolina, "Esse quam videri,": "To be rather than to seem." Requiring companies to have a privacy policy readily available to the general public, and forcing them to abide by that policy, is both reasonable and logical. To force companies to deliver up to four different notices at four different times to a single individual (as with CCPA) only increases burdens on businesses and the general apathy of individuals.

6) Private Rights of Action

A final badge noted above for First Wave rules is the lack of a private right of action permitting individuals to sue businesses for failure to meet regulatory requirements. While GDPR created such a right of action,[75] CCPA permits private claims only under its security provisions.[76] Whether to include private rights of action is now more a political food fight than a field for thoughtful debate. Note that if penalties become draconian, actors may become overly conservative, and fear of liability could squelch the offering of valuable services, or creative uses of data, that benefit everyone.

Other Concerns and Modest Proposals

In addition to the above concerns that current regulatory schema have brought to light, there are other areas that should be considered in creating a way forward.

Technology, Including DLT

Any proposed regulations should very much consider the exponential pace of technological development[77] and upcoming technologies. Unfortunately, the Second Wave of regulations, including those currently proposed in Congress, tend to hamstring development and make implementation of certain new tools such as DLT difficult.

An alternative: Broad exemptions, or at a minimum an exemption process, for new technologies should be built into legislation, permitting future companies to implement technology based on a review of potential impacts on individuals and society. While GDPR requires that controllers undertake a data protection impact assessment and consult with supervisory authorities, it is an additional *requirement* rather than an *exemption*. Permitting a process for public review, publication of an impact assessment and implementation of new technology together with clear, reasonable and widely accepted limitations may help these regulations to gain favor and protect both the economy and privacy. More broadly, however, technology is short-lived and constantly evolving. Regulations can be much more long-lived and change more slowly. As such, they must either allow for greater latitude for change (e.g., by building in sophisticated exceptions for new technologies on the horizon, such as quantum computing, AI and DLT) or accelerate their own change with mechanisms such as sunset provisions.[78]

The Pandemic

COVID-19 and governmental responses are bringing privacy concerns to the fore. Often the discussion is posed as weighing privacy against public health, such as in the context of monitoring individuals' movements.[79] Ultimately, some difficult decisions must be made in how to weigh public safety against privacy. While far beyond the scope of this article, HIPAA has proven problematic in this context. For example, HIPAA generally relies on reporting to governmental units of outbreaks and public concerns. COVID-19 has overwhelmed those agencies, and they have understandably been slow to provide individuals with needed information. In certain situations, covered entities have chosen to abide by their understanding of HIPAA regardless of consequences, e.g., refusing to disclose information, or even requesting authorizations from patients, in situations where their actions endanger the safety of numerous individuals.[80]

In short, in the 20 years since the release of the "final" HIPAA privacy regulations, there have been revealed a myriad of weaknesses of the regulations. COVID-19 made the potential impact obvious and poignant in just a matter of weeks.

Conclusion

Privacy and security requirements can be greatly improved. Unfortunately, there is little reason to believe that any current proposals will materially improve HIPAA, nor is there reason to believe that they pose a likelihood of long-term success. The problem with these attempts is neither a lack of will, nor a lack of debate. The problem appears to be a lack of understanding

and creativity. Legislators and agencies, working with stakeholders, can improve privacy and create room for progress, but only by taking a step back, bringing in unbiased experts in technology and human needs, and respecting the obligations each of us carries to value each other's confidences, personhood and freedoms.

Whether HIPAA can be saved must be answered as both "*absolutely yes*" and "*absolutely no.*" The "yes" is clear insofar as HIPAA has become synonymous with the protection of privacy. That legacy should, and likely will, be preserved. HIPAA can be saved, as well, by new laws that broaden the privacy and security of health information. The "no," however, is that HIPAA reflects a now antiquated view of what must be protected (only health information, narrowly defined, when held by a narrow band of actors), belief by Congress that health information should be treated differently from other sensitive information, and trust by society that reasonable providers applying reasonable security measures will adequately protect our data. The hard-to-avoid conclusion is that neither the First Wave nor Second Wave approaches will adequately address current and future privacy and security concerns, which leaves only one hope: that a radical shift in thinking can lead to a broader, more inclusive and more realistic Third Wave — a wave to carry us forward into a new understanding of privacy and the role of government in protecting our most intimate possession.

1 Pub.L. 104-191, 110 Stat. 1936, August 21, 1996.

2 In 1994, electronic processing of claims accounted for less than half of all transactions. Between 2004 and 2017 electronic health record (EHR) adoption increased from 20.8% to 86.9%, with a major jump between 2011 and 2013, likely impacted by the HITECH provisions of the American Recovery and Reinvestment Act of 2009, which required Stage 1 meaningful use attestation beginning in 2011.

3 *Four years later*, in September 2000, the Office of the Assistant Secretary for Planning and Evaluation, U.S. Department of Health & Human Services, Frequently Asked Questions about Electronic Transaction Standards Adopted under HIPAA (ASPE FAQs) https://aspe.hhs.gov/report/frequently-asked-questions-about-electronic-transaction-standards-adopted-under-hipaa included the question, "Does the law require physicians to buy computers?"

4 ASPE FAQs.

5 Determining the total amount of savings brought about by these rules, known as the Transaction Rules, is difficult. The American Medical Association (AMA), however, has stated that physicians utilizing HIPAA standard electronic transactions are "saving thousands of dollars annually." *See* https://assets.ama-assn.org/resources/images/psa/hipaa-tcs.pdf.

6 *See* comments from the Centers for Medicare & Medicaid Services, with the publication of the final security rule, 68 Fed. Reg. No. 34, 8334 (Feb. 20, 2003) Section I.

7 45 C.F.R. Part 164, Subpart C.

8 *Id.*

9 *See* Conn, J., "HIPAA, 10 years after," *Modern Healthcare*, Aug. 7, 2006, https://www.modernhealthcare.com/article/20060807/NEWS/608070324/hipaa-10-years-after ("while privacy and confidentiality of patient data has always been important to AHIMA members, HIPAA 'pushed it to the front of the brain on day-to-day issues'"). The privacy provision of HIPAA was added during a time when a stand-alone health privacy law was being reviewed in the Senate but did not look like it would make it out of committee. Lechner, "How did we get a health privacy law?" *Quill*, Sept. 23, 2003.

10 *Money Magazine*, Aug. 1997, as reported by the Electronic Privacy Information Center, https://epic.org/privacy/survey/ and Privacy Rights Clearinghouse, https://privacyrights.org/resources/public-attitudes-about-privacy-information.

11 https://morningconsult.com/2019/12/18/most-voters-say-congress-should-make-privacy-legislation-a-priority-next-year/.

12 Pub.L. 106-102, 113 Stat. 1338 (Nov. 12, 1999).

13 One might also include among this First Wave of statutes governing privacy or the sense of privacy: the Children's Online Privacy Protection Act (COPPA), Pub.L. 105-277, 112 Stat 2681-728 (Oct. 21, 1998); the Controlling the Assault of Non-Solicited Pornography And Marketing (CAN-SPAM) Act of 2003, Pub.L. 108-187, 117 Stat. 2699 (Dec. 16, 2003); and the Telephone Consumer Protection Act of 1991 (TCPA), Pub.L. 102-243, 105 Stat. 2402 (Dec. 20, 1991).

14 These badges are likely influenced by the Federal Trade Commission (FTC) Fair Information Practice Principles, as provided in a Report to Congress dated June 1998, https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf. These principles include notice/awareness, choice/consent, access/participation, integrity/security and enforcement redress.

15 Though as noted below these were more specific than security requirements in later statutes and regulations.

16 To be more exact, the HIPAA Security Rule makes encryption "addressable." HIPAA's Breach Notification Rule at 45 C.F.R. Part 164, Subpart D applies only to "unsecured protected health information." Health records that are encrypted in accordance with NIST standards are considered secured and not subject to the Breach Notification Rule (assuming at the time of a breach the PHI could not be accessed in a readable format).

17 45 C.F.R. § 164.506(b) provides that a covered entity "*may*" obtain consent of an individual to use or disclose PHI for treatment, payment and healthcare operations. Consent is not mandatory. This consent is distinct from the ability of an individual to "authorize" uses and disclosures of PHI.

18 In the case of healthcare providers, it is further limited to those that transmit health information in electronic form in connection with a transaction covered by the Administrative Simplification rules. "Health care clearinghouses" are entities that translate health information from nonstandard formats into standard data elements or vice versa.

19 *See* comments from HHS with first final HIPAA Privacy Rule, 65 Fed. Reg. 68 No. 250, 82471 (Dec. 28, 2000).

20 The Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of the American Recovery and Reinvestment Act of 2009 (Pub.L. 111-5), Section 13404 made the HIPAA Security Rule, the obligations required to be in a business associate agreement, and relevant provisions of the HITECH Act applicable directly to business associates.

21 Though such sale, use, disclosure, etc. may be subject to other limitations, e.g., under state law or FTC limitations.

22 68 Fed. Reg. No. 34, 8335.

23 "Equally," in this sense, relates to the cost for hiring professionals and undertaking universal requirements. In some cases, smaller entities may have additional burdens in locating resources or creating a compliance program, whereas larger entities may have such assets at hand.

24 At least theoretically, if required to protect against reasonable threats, an entity may be mandated to adopt measures not listed in the HIPAA Security Rule. One example could be adoption of a vendor assessment program, which is a staple of security compliance programs but completely omitted from HIPAA Security Rule requirements.

25 45 C.F.R. § 164.308.

26 45 C.F.R. § 164.312.

27 45 C.F.R. § 164.310.

28 *See,* for example, various settlements with the Office for Civil Rights (OCR) relating to failure to conduct a risk assessment or implement sufficient administrative protections. https://www.hhs.gov/about/news/2020/03/03/health-care-provider-pays-100000-settlement-ocr-failing-implement-hipaa.html ($100,000 settlement with a physician practice for failure to conduct a risk analysis); https://www.hhs.gov/about/news/2017/04/12/overlooking-risks-leads-to-breach-settlement.html ($400,000 settlement with a federally qualified health center for lack of risk analysis or implementation of risk management plan). Much larger settlements have been entered into with larger covered entities, ranging up to $16 million.

29 There are a handful of automated approaches to HIPAA compliance that claim to be less expensive yet customized to the client. For purposes of full disclosure, one such product is HIPAA2Z™ (www.hipaa2z.com), which is a HIPAA privacy and security compliance platform developed by the author.

30 The author is not aware of any surveys of how often covered entities receive requests under these rights, but anecdotally is aware of Fortune 100 covered entities that annually receive less than 10 of most of these types of requests.

31 There are four narrow exceptions of types of information that are not considered PHI but otherwise meet the definition.

32 45 C.F.R. §§ 164.502(d)(2) and 164.514(a).

33 45 C.F.R. § 164.514(b).

34 The alternative method involves acquiring the certification of an expert that the risk is very small that the information could be used to identify an individual.

35 https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html.

36 "Ransomware" is a general term for a broad variety of malicious software. In some cases, a ransomware attack may involve access to, or exfiltration of, information.

37 A ransomware attack would, however, meet the definition of a "security incident," which requires implementing response and reporting procedures. *See* 45 C.F.R. § 164.304.

38 https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.

39 *Id.* Emphasis added.

40 https://www.hhs.gov/hipaa/for-professionals/faq/2074/may-a-business-associate-of-a-hipaa-covered-entity-block-or-terminate-access/index.html?language=es.

41 A nefarious cloud service user with no intent to pay its bill theoretically could request that the cloud provider execute a business associate agreement, though not storing PHI with the provider, knowing that the cloud provider would be forced to return the user's data even if payment was not made under the assumption that PHI was involved.

42 Each has received such treatment. *See*, for example, Epstein, Wyman and Wilkinson, "Blockchain Meets Healthcare: Understanding the Business Model and Implementing Initiatives," ACC Docket, Aug. 28, 2017,

https://www.nelsonmullins.com/storage/4db2ba62b5531942d89ab659e2921280.pdf; Bass, Todaro, Epstein and Wyman, "Blockchain In Healthcare: An Executive Update," Health IT Outcomes, Feb. 15, 2017, https://www.healthitoutcomes.com/doc/blockchain-in-healthcare-an-executive-update-0001; Wyman, "Navigating the Risks of New Healthcare Technologies," Nashville Medical News, July 16, 2019, https://www.nashvillemedicalnews.com/navigating-the-risks-of-new-healthcare-technologies-cms-3148.

43 Such is the hope. *See* Falkon, "The Story of the DAO — Its History and Consequences" The Startup, Medium, Dec. 24, 2017, https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee.

44 *See supra* n. 42, Epstein, Wyman and Wilkinson.

45 It is very unlikely that an EHR will ever be fully housed in a distributed ledger, as DLT technology does not permit holding large amounts of information, and the technology is comparatively slow. As such, DLT would likely use encrypted "pointers" to non-Blockchain EHR databases. For further discussion, *see supra* n. 42, Epstein, Wyman and Wilkinson as to why HIPAA currently permits most Blockchain use cases in healthcare.

46 EU 2016/679.

47 CA Civil Code Title 1.81.5 added by Stats. 2018, Ch. 55, Sec. 3, codified at Cal. Civ. Code 1798.100-1798.199.

48 *See* Bennett, Bertin, Cooper, Kostka, Nash, Nonaka and Van Quathem, "The GDPR and Blockchain," Inside Privacy, July 24, 2018, https://www.insideprivacy.com/international/european-union/the-gdpr-and-blockchain/; "GDPR, CCPA, Blockchain and Renewable Energy: Policy Lagging Behind Technology" The National Law Review, Feb. 1, 2019, https://www.natlawreview.com/article/gdpr-ccpa-blockchain-and-renewable-energy-policy-lagging-behind-technology.

49 For example, by using entangled particles such that any attempt by a third party to intercept a message would immediately cause the particles' quantum state to collapse and reveal the interception.

50 Varmeer, Peet, Securing Communications in the Quantum Computing Age, https://www.rand.org/pubs/research_reports/RR3102.html.

51 In 1997, Dr. Latanya Sweeney, using an insurance data set that had been stripped of direct identifiers, identified Massachusetts Governor William Weld within a public data set, primarily by utilizing publicly-available Cambridge voting records. While this re-identification received much publicity, it appears that such a feat, at least at the time, could not easily have been replicated for less-famous individuals not already known to be in the relevant data set. *See* Barth-Jones, "The "Re-identification" of Governor William Weld's Medical Information: A Critical Re-examination of Health Data Identification Risks and Privacy Protections, Then and Now," SSRN, June 4, 2012, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2076397.

52 https://www.infosecurity-magazine.com/news/netflix-second-data-challenge-on-revealing/.

53 Yoo, J.S., Thaler, A., Sweeney, L., & Zang, J. (2018), Risks to Patient Privacy: A Re-identification of Patients in Maine and Vermont Statewide Hospital Data, *Technology Science,* https://techscience.org/a/2018100901/; Na, L., Yang, C., Lo, C.C., Zhao, F., Fukuoka, Y., & Aswani, A. (2018), Feasibility of Reidentifying Individuals in Large National Physical Activity Data Sets From Which Protected Health Information Has Been Removed With Use of Machine Learning, *Journal of the American Medical Association,* https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2719130; Cohen, J.K. (2019), *AI can re-identify de-identified health data, study finds,* https://www.beckershospitalreview.com/artificial-intelligence/ai-can-re-identify-de-identified-health-data-study-finds.html.

54 The applications were ultimately denied on April 29, 2020, not because the inventions themselves were not patentable, but because there was not listed a "natural person" as the inventor. https://www.uspto.gov/sites/default/files/documents/16524350_22apr2020.pdf?utm_campaign=subscriptioncenter&utm_content=&utm_medium=email&utm_name=&utm_source=govdelivery&utm_term=.

55 As partially detailed above, HHS and OCR have continued to evolve approaches and address new issues. The regulations themselves have not been subject to significant revisions since publication of HITECH-related modifications in early 2013. 78 Fed. Reg. No. 17, 5566 (Jan. 25, 2013).

56 N.Y. Gen Bus. Law 899-bb.

57 GDPR Article 4(7).

58 GDPR Article 4(11).

59 One might argue that GDPR *security* requirements (Articles 32 – 34) are much looser than those within HIPAA. Activities required under GDPR also can vary to a degree based on an entity's size and the nature of its business.

60 CA Attorney General Final Text of Regulation (Jun. 1, 2020) Article 2, Section 999.304 – 308.

61 *See*, for example, S.3456, Consumer Data Privacy and Security Act of 2020 (CDPSA), https://www.congress.gov/bill/116th-congress/senate-bill/3456/text#toc-ida36d4215c4c7482797c049d449e342d7; S.2986, Consumer Online Privacy Rights Act (COPRA), https://www.congress.gov/bill/116th-congress/senate-bill/2968/text; United States Consumer Data Privacy Act of 2019 Staff Discussion Draft introduced by Sen. Roger Wicker (CDPA), https://aboutblaw.com/NaZ; and the draft bill released by staff for the House Energy and Commerce Committee (Energy Bill), https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2019/12/2019.12.18-Privacy-Bipartsian-Staff-Discussion-Draft.pdf. Discussions of the above relate to proposals or bills as initially submitted or released and may not take into account revisions.

62 15 U.S.C. § 41 et seq.

63 The CDPA also would not preempt HIPAA, and the Energy Bill is currently silent on the question.

64 Among the largest cloud providers, as of the date of this article, the following entities had the following total market capitalization (rounded): AWS (Amazon): 1.14 Trillion; Azure (Microsoft): 1.3 Trillion; Google Cloud (Google): 1.3 Trillion; IBM Cloud (IBM): 122 Billion.

65 These concepts are defined in various ways among various bills and rules, e.g., "controller" (GDPR) "business" (CCPA) or "covered entity" (various proposed rules).

66 *See supra* n. 55.

67 An issue could arise if the bare holding of information by Company B is a concern, e.g., embarrassing or commercially sensitive information that cannot be "unseen." Sufficient safeguards could be introduced to address this unusual scenario.

68 For a further discussion, *see* Kosseff, "Congress Is Finally Tackling Privacy! Now Let's Do Cybersecurity," Slate, Dec. 3, 2019, https://slate.com/technology/2019/12/congress-national-privacy-law-cybersecurity.html.

69 CDPSA Section 6.

70 State of California, Department of Finance Economic and Fiscal Impact Statement, (EFIS) https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-std399.pdf. The estimate also estimated statewide benefits from expanded "legal and IT related compliance services in CA."

71 State of California Department of Justice, Office of the Attorney General, Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations, Prepared by Berkeley Economic Advising and Research, LLC, Aug. 2019, https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf.

72 *See supra* n. 10 and 11.

73 For a high-level discussion of price transparency and its failure to impact consumer buying in healthcare, *see* "Will Price Transparency in Health Care Lower Costs or Backfire? Knowledge@Wharton, July 2, 2019. https://knowledge.wharton.upenn.edu/article/will-price-transparency-health-care-lower-costs-backfire/

74 *See* Kint, "Is it Time to Rethink Notice and Choice as a Fair Information Privacy Practice?" Cyber Law Monitor, Feb. 13, 2019, https://www.cyberlawmonitor.com/2019/02/13/is-it-time-to-rethink-notice-and-choice-as-a-fair-information-privacy-practice/. Note, however, that requirements for notices do have an advantage insofar as enforcement agencies may hold companies accountable for failure to meet the standards set forth in their privacy policies. One may also argue, however, that this "advantage" encourages businesses to either not have any privacy policy or, where required, make them as vanilla and filled with caveats as possible.

75 GDPR, Article 79.

76 CCPA 1798.150.

77 One may argue that Moore's Law (that the number of transistors on a microchip doubles every two years) is slowing (as was inevitable). The broader belief that "technology" (when defined broadly) is growing exponentially may be a bit vague but has support. Should Neven's law regarding quantum computing prove true, the rate of technological advancement going forward may prove to be doubly exponential. *See*, generally, Hartnett, "A New Law to Describe Quantum Computing's Rise?" Quanta Magazine, June 18, 2019, https://www.quantamagazine.org/does-nevens-law-describe-quantum-computings-rise-20190618/.

78 *See* Epstein, Wyman and Wilkinson, n. 42 *supra,* p. 64, for a brief discussion on how smart contracts might impact and improve regulatory processes. Other approaches might include sunset provisions that force regulators and/or legislators to regularly reassess current technologies and related statutory and regulatory schemes.

79 On May 7, 2020 U.S. Sens. Wicker, Thune, Moran and Blackburn introduced the "COVID-19 Consumer Data Protection Act," https://www.commerce.senate.gov/services/files/A377AEEB-464E-4D5E-BFB8-11003149B6E0. The Act relies on the same Second Wave assumptions and approaches described above, e.g., reliance on notice, a privacy policy and active consent, definitions of "aggregate" and "de-identified" data, and personal rights to deletion or de-identification and data minimization.

80 These situations were not addressed in guidance from HHS relaxing enforcement of HIPAA rules due to COVID-19. This situation was not made better by GDPR in the European Union, as various supervisory authorities released contrary statements on issues such as the ability to take employees' temperatures.

About the Author

Roy Wyman is co-chair of the Privacy & Security Industry Group and a member of the firm's Technology, Outsourcing and Privacy Practice Team at Nelson Mullins. He assists clients in addressing data and regulatory concerns, loss of data, privacy and cybersecurity issues arising under HIPAA, GDPR, TCPA, CAN-SPAM, CCPA and other statutes, the review of legal implications of new technologies, and implementation of processes to address regulatory concerns. He may be reached at roy.wyman@nelsonmullins.com.

ABA American Bar Association | /content/aba-cms-dotorg/en/groups/health_law/publications/health_lawyer_home/2020-august/can-hip