Update On Draft Commentary on the Privacy and Security of Emerging Health Data (April 2024)

Update On Draft Commentary on the Privacy and Security of Emerging Health Data (April 2024)

Drafting Team Members:

Sara Romine (Drafting Team Leader)
Maureen Brady
Chris Cronin
Austin Moore
Corban Rhodes
Jami Vibbert
Colman McCarthy (Steering Committee Liaison)
Dalia Ritvo (Steering Committee Liaison)

UPDATE ON DRAFT COMMENTARY ON THE PRIVACY AND SECURITY OF EMERGING HEALTH DATA

April 2024 for Review and Comment by Working Group 11

All:

We received considerable feedback on the first draft commentary on whether HIPAA adequately covers consumer health and non-traditional health data both during and after the Tampa WG11 meeting. As a result of that feedback, we began to pivot toward a different type of commentary and want to use this meeting to determine whether (1) the current direction is both viable and valuable; or (2) we should go back to a brainstorming group to reboot the commentary in a potential different direction (or something in between). We are also considering whether we need additional team members to assist with the drafting.

To aid in our discussion, below is both a short outline detailing the current direction of the drafting team and the draft commentary that emerged out of the Tampa meeting. The group plans to use substantial parts of the existing draft commentary to build out the current outline, but the critical question is whether this team should propose a legislative framework for addressing private health data.

We look forward to your comments.

A. The need to develop an evolved legal framework for addressing private health data.

1. Practical problems and limitations in the current federal legal framework.
    a. What's good in HIPAA
    b. What's bad or inadequate about HIPAA.
        i. Definition of PHI
        ii. Issues with scope

B. Guiding principles for development of an evolved framework for health data.

1. What should be considered health information (is a tiered approach to data sensitivity appropriate?)
    a. Utility of the information/driver of medical research
        i. Sensitivity of it.
            1. Need for consent and transparency where highly sensitive.
2. Suggestions for implementing a legislative framework—what are the guiding principles?
    a. What would the litigation landscape look like here?
        i. How do you cut out lawsuits over ticky-tacky violations that don't necessarily trigger sensitive data (example given that may be subject to debate--data breach lawsuits over appointment reminders)?
        ii. How do you incentivize the right behavior?

DRAFT COMMENTARY ON WHETHER HIPAA ADEQUATELY COVERS CONSUMER HEALTH AND NON-TRADITIONAL HEALTH DATA

November 2023 for Review and Comment by Working Group 11

I. Introduction and Purpose

[insert coming]

II. U.S. Health Privacy Regulation is Patchworked and only Infrequently and Informally Updated

A. HIPAA

The Health Insurance Portability and Accountability Act was initially passed in 1996. It has only been substantially amended once since, by the Genetic Information Nondiscrimination Act and Health Information Technology for Economic and Clinical Health Act (as enacted in the American Recovery and Reinvestment Act of 2009). In much of its substance, Privacy, Security, and Breach Notification Rules, as implemented by regulation, have been unmodified for more than a decade.

Rather than adhere to a more formal legislative or regulatory rulemaking process, HHS has largely sought to evolve its interpretation and application of the regulation through guidance and enforcement. While these mechanisms are more flexible, they sometimes lack the clarity and transparency afforded by alternative processes (which create public commentary, legislative commentary, and other artifacts that are useful to regulated entities, to say nothing of bright-line rules). In some cases, this has been met with active criticism.

On May 22, 2023, the American Hospital Association ("**AHA**") published a letter related to HHS regulatory activities.[1] In its first part, the letter was supportive of the notice of proposed rulemaking ("**NPRM**") issued by the agency with respect to Reproductive Health Care, issued on April 12, 2023.[2] Sensitive to the then-recent *Dobbs* decision from the United States Supreme Court, the AHA letter noted that the proposed rule would "enhance provider-patient relationships by providing heightened privacy protections for information about care that is lawful under the circumstances in which it is provided, but may nonetheless get swept up in criminal, civil or administrative investigations."[3] Conversely, the rule pushed back on the agency's December 2022 guidance[4] relating to tracking technology. Among a litany of other concerns, the letter criticizes the guidance for dramatically expanding the definition of protected health information ("**PHI**") well beyond the scope established by the regulation and intent of regulators.

To-date, HHS has neither announced enforcement against its tracking technology guidance nor adopted its proposed rule on reproductive privacy.

B. State Medical Privacy, Consumer Privacy, and Breach Notification Laws

[1] https://www.aha.org/lettercomment/2023-05-22-aha-letter-ocr-hipaa-privacy-rule-online-tracking-guidance
[2] https://www.hhs.gov/hipaa/for-professionals/regulatory-initiatives/hipaa-reproductive-health-fact-sheet/index.html
[3] Ibid 1
[4] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html

Several state laws protect the privacy of medical information.[5] Of these, the California Confidentiality of Medical Information Act ("**CMIA**") is among the most comprehensive. While the CMIA is the focus of discussion in this subsection, other states have enacted their own medical privacy laws that may have similarities but also differences in scope, penalties, and exceptions.

The CMIA primarily protects the privacy of patients by prohibiting unauthorized disclosure of medical information by healthcare providers, health plans, and contractors without the patient's written consent. The CMIA applies to various entities including healthcare providers (like doctors, clinics, and hospitals), health insurance companies, and contractors or businesses that receive medical information. Medical information can't be shared, sold, or otherwise disclosed without the patient's written consent. There are some exceptions, such as when disclosure is needed for treatment, payment, or healthcare operations or is mandated by law.

Unauthorized disclosure can result in both civil and criminal penalties under the CMIA. This includes nominal damages, actual damages, and potential punitive damages. Fines can be substantial, especially in cases where there's a pattern of violations. With the rise of electronic health records (EHR), the CMIA has provisions that specifically address the confidentiality of electronic medical information. These provisions set standards for ensuring the confidentiality and integrity of electronic medical records. While the CMIA is strict, there are situations where medical information can be disclosed without explicit patient consent. These situations include, but aren't limited to, judicial proceedings, certain research activities, and public health requirements. HIPAA also provides standards for medical privacy. Where both HIPAA and the CMIA apply, healthcare entities must comply with the stricter standard of the two.

In addition to state laws focusing specifically on the privacy of medical information, a growing body of state consumer privacy laws and breach notification requirements is also impacting organizations' treatment of health information (although many expressly exempt organizations covered by HIPAA in various forms)[6]. There are currently 54 state and territorial breach notification laws and, while early legislation had primarily targeted sensitive data elements like financial account information, Social Security numbers, and drivers' license numbers, an increasing number also require notification for categories of insurance, genetic, or other health and medical information. Similarly, the CCPA/CPRA and other state laws also expressly regulate categories of health and medical information. In many instances, however, these laws were drafted primarily with an eye to broader consumer privacy issues, such as those arising through search engines and social media.[7] As such, they currently lack HIPAA's sensitivity to the health care context as embodied in uses and disclosures described by the regulation (e.g., "health care operations"), commentary in the Federal Register, and decades of guidance and enforcement.

C. FTC Act and Health Breach Notification Rule

Paradoxically, the FTC has risen to become both the country's most aggressive privacy enforcement agency **[cite $bn enforcement cases]** as well as the agency with the broadest – and vaguest – authority to take enforcement action on consumer privacy and data protection harms. The FTC's legislative authority to seek penalties in that space derives entirely from Section 5 of the FTC Act of 1914, which prohibits "unfair and deceptive acts and practices".**[cite]** While the FTC has sought to clarify this authority through guidance and enforcement, the legislative underpinnings granting it authority have

[5] **[add cite to other state laws, inc Texas]**
[6] [Insert cite to exemptions]
[7] https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html

remained substantially unmodified for more than a century, although the Health Breach Notification Rule, passed as part of HITECH, did enhance its coverage of breach incidents. The FTC appears to recognize the complexities and ambiguities created by the federal government's treatment of health information privacy, and has drafted guidance aimed at resolving confusion among regulated entities.[8]

III. Health Information Processing Activities and Technologies Continue to Change Rapidly

Despite the cardinal rule of "Thou shalt not Google" many people first turn to Google, rather than their traditional medical provider, for a quick diagnosis of medical and health symptoms. So often Google directs to the most extreme and rare interpretation of the symptoms. In other words, people with symptoms of a colds come away with diagnoses of anything from a rare form of cancer to brain tumors. But the primary issue that should be asked, was that diagnosis and interpretation of symptoms from a physician patient relationship OR is the information provided to the medical websites.

With the advancement in medical technologies there has been a growth in computer-based programming and applications that gather and store medical information as well as personal information. In some instances, the applications will issue suggested diagnoses or symptom matching programs. (*i.e.* WedMD's and Mayo Clinic's "Symptom Checker.") However, these applications are not covered by HIPAA.

Against the backdrop of a patchworked U.S. health care privacy landscape, and the often infrequent and informal means by which it is updated, health care technologies and practices have continued to develop at a rapid pace. A sampling of developments with significant privacy impacts – to which privacy laws and requirements are in many instances still playing catch-up – is given below:

A. Statistical Re-Identification

HIPAA's "Safe Harbor" standard outlines a set list of identifying data elements that entities regulated by HIPAA can remove in order for information to be rendered "de-identified" for the purposes of HIPAA. "De-identified" information is no longer treated as PHI, meaning that it can be used without regard for the regulation's requirements and restrictions (a similar condition to the treatment of "anonymous" information under the GDPR and other regulations). This standard is currently more than a decade old, however, and the science of re-identification has continued to advance in the meantime. A study published in 2017[9] found that information de-identified under the Safe Harbor standard was able to be re-identified by name and address with respect to approximately a quarter of the population whose information had been de-identified. This should create significant doubt as to the continued privacy-preserving value of the standard.

B. Genetic Re-identification

With the advent of companies like 23andMe and Ancestry.com, individuals are able to gather genetic information on themselves and make connections with others that share their DNA. This has made guaranteeing the anonymity of sperm donors a near impossibility.[10] Given the sensitivity that many feel around sperm donation, this development threatens to seriously chill donor participation with cryobanks, with downstream impacts on individuals seeking fertility assistance from these organizations.

[8] https://www.ftc.gov/business-guidance/resources/collecting-using-or-sharing-consumer-health-information-look-hipaa-ftc-act-health-breach
[9] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6344041/
[10] https://www.scientificamerican.com/article/consumer-dna-tests-negate-sperm-bank-donor-anonymity/

C. Artificial Intelligence and Machine Learning

HHS broadly has provided commentary on the opportunities in this space (e.g., link) but OCR, on an initial review, has not provided comprehensive commentary on acceptable practices for covered entities to follow vis-à-vis HIPAA compliance.

D. Telehealth

HIPAA draws no distinction between written and oral medical records and information. Whether PHI is collected through in person visits with a health care provider or via phone or video technology, the same rules and regulations apply to the gathering, storing, and disclosure of PHI. Nonetheless, the covered entity is still required to do a risk analysis of the technologies used to provide telehealth services. Risk of interception, lack of encryption, or breach of the stored or gathered information must all be considered by the health care provider prior to engaging patients in telehealth services.

Often the risk of compromise outweighs the use of telehealth services if the health care provider is not equipped to update and oversee the ever-changing technologies. While telehealth can significantly expand access to health care, certain populations may have difficulty accessing or be unable to access technologies used for audio-video telehealth because of various factors, including financial resources, limited English proficiency, disability, internet access, availability of sufficient broadband, and cell coverage in the geographic area. Audio-only telehealth, especially using technologies that do not require broadband availability, can help address the needs of some of these individuals.

E. Data Sharing and Portability

HIPAA was designed for this very purpose. The rules and regulations of HIPAA account for the necessity to share data and information between the patient and health care providers as well as allowing the data to be portable for the patient's benefit. The guidance from HHS is clear: follow the rules of HIPAA. Data sharing and portability by the covered entity is regulated. Data sharing and portability by the patient would be voluntary and would not be subject to HIPAA laws. Individuals who wish to collect and share information on their own do so at their own risk. The covered entity that gave the patient the medical information would have an obligation to secure the information within its care and in the transmission of the information outside of its facility. This means that if a patient were to obtain his/her medical records and they were placed on a thumb drive by the covered entity, once received by the patient, any use or disclosure is out of the hands of the covered entity.

F. Wearables

Wearables, like other tracking technology, are regulated only if the data is collected by a covered-entity. Data that is collected and stored with a technology company, such as Apple's HealthApp, would not be subject to privacy laws and regulations. Tracking technologies collect information and track users in various ways, many of which are not apparent to the website or mobile app user. Websites commonly use tracking technologies such as cookies, web beacons or tracking pixels, session replay scripts, and fingerprinting scripts to track and collect information from users. Mobile apps generally include/embed tracking code within the app to enable the app to collect information directly provided by the user, and apps may also capture the user's mobile device-related information. For example, mobile apps may use a unique identifier from the app user's mobile device, such as a device ID or advertising ID. These unique identifiers, along with any other information collected by the app, enable the mobile app owner or vendor

or any other third party who receives such information to create individual profiles about each app user.

Health information is now captured in apps that are not covered by HIPAA because the app is not acting as a covered entity or business associate. Individuals may not realize that the information they are providing could be considered health information or do not care due to the convenience of the application they are wanting to use. However, when and if a breach of that data occurs, the individuals may require more protections around the applications, which may initiate more amendments to the rule to possible incorporate the products that collect such data into HIPAA.

Regulated entities disclose a variety of information to tracking technology vendors through tracking technologies placed on a regulated entity's website or mobile app, including individually identifiable health information (IIHI) that the individual provides when they use regulated entities' websites or mobile apps. This information might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, or any unique identifying code. All such IIHI collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services. This is because, when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (*i.e.*, it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care.

IV. Are HIPAA Security Rule Specifications Out of Date and Should They Be Updated?

The HIPAA Security Rule specifications were originally finalized in 2003[11], and were updated most recently in 2013 in the Omnibus Rule[12]. The rule's specifications were written at a time when information security risks and their mitigating controls were much different than they are twenty years later. Regulatory experts and advocates have argued[13] that the Department of Health and Human Services (DHHS) Office for Civil Rights (OCR) should update the HIPAA Security Rule's specifications for security controls, so they are more relevant to current threats and standards of care. Such arguments describe the advanced complexity and presence of computer technologies used to handle protected health information while also describing continuously evolving information security attack methods and tools that are used to prevent them.[14] An assumption seems to underlie these arguments; that regulators should provide the standard of care that covered entities must follow. We believe that this assumption is both impractical and wrong for the following reasons.

- **Futility**. The pace of regulatory change will always be slower than the pace of evolution of information security threats and safeguards.

- **Limitations of Rulemaking**. Unless legislation permits otherwise, U.S. regulators are constitutionally unable to demand specific safeguards of covered entities. This is certainly the case with the HIPAA Security Rule. However, we do recommend that DHHS help covered entities better understand how to use existing specifications in the Security Rule to stay current with contemporary information security risks and safeguards.

[11] Citation
[12] Citation
[13] Site examples
[14] Cite

The following sections explore the limitations on updating the HIPAA Security Rule's specifications further.

A. Futility

The pace of regulatory rulemaking is very slow, and much slower than the development of new information technologies that handle PHI, the methods for compromising those technologies, and the safeguards that prevent those new attacks.

Five years passed between HIPAA's statutory enactment[15] in 1998 and the publication of the Security Rule in 2003[16]. An additional six years passed between the publication of the Security Rule and the HITECH Act[17] in 2009 that updated the Security Rule. And finally, the Omnibus Rule[18] was published four years later in 2013 and is the version of HIPAA that remains current today[19].

Since 2013 information technologies that handle PHI have significantly advanced. Some brief examples are:

1. Internet of Medical Things (IoMT) is a field of technology that gathers, transmits, and stores information about the patients who are attached to (or who use) that technology, most often over wireless networks. The technology helps patients, clinicians, and researchers understand and improve health, and at the same time creates a broader attack surface for hackers[20].
2. Telemedicine has permitted clinicians to interact directly with patients over networked applications over long distances. This provides patients with access to medical care, while also creating more opportunities for hackers to attack telemedicine systems and applications to gather patient and insurance information[21].
3. Artificial Intelligence is increasingly used in clinical environments to assist in decision-making, but carries with it data integrity issues (are clinicians using information that is consistent with the facts, citations, and current science and technology?) and confidentiality issues (are questions being asked of AI systems and ingested in AI systems that could identify the patient? Is patient information being used to train AI?)[22].

Threats that have developed since the 2013 Omnibus rule are no less impressive:

- Ransomware has escalated notably in clinical environments, seizing patient data as well as encrypting it, creating availability and confidentiality threats.
- Technology features that are intended to improve analytics and marketability of patient choices (such as web pixel tools) become opportunities for privacy violations and security violations when organizations fail to see the acquired information as PHI.

And the nature of threats involved in third parties has evolved to the point where business associate agreements are no longer plausibly enforceable.

- Health tracking apps that interact with insurance carriers and clinical providers are vulnerable to attack and use constantly evolving technologies that would be impossible for their customers to monitor and control.

---

[15] Cote 1999
[16] Cite 2004
[17] Cite 2009
[18] Cite 2013
[19] But for regulatory guidance and clarification, such as the [acknowledgement that the Secretary may consider adherence to a security standard as a mitigating factor when breaches occur – Cite].
[20] What security threats are targeting IoMT devices (and how to prevent being hacked) | Nuspire
[21] 2019 Healthcare Data Breach Report (hipaajournal.com)
[22] The rise of artificial intelligence in healthcare applications - PMC (nih.gov)

- The growth in cloud services – which are themselves built from a supply-chain of many other third parties – are increasingly relied upon by health information systems at payers and provides. These cannot be plausibly monitored or controlled by clinicians or insurance carriers.

The rapid development of information technologies and of threats to those technologies make it implausible for regulations to keep up.

B. Limitations of Rulemaking

Regulators, such as DHHS, issue rules through a set of processes set by the Office of Management and Budget (OMB). Each regulatory agency as well has its own rules and procedure for rulemaking. But what they all have in common is the degree to which they both independently from and in deference to legislation. Because regulators operate within the Executive branch, their powers to create requirements in regulations are limited to the degree that they either contradict or go beyond legislated statutes. Congress delegates rulemaking authority to executive agencies because statutes are neither specific enough to describe how regulations can be enforced, nor informed enough to understand how industries covered by regulations can comply with regulations[23]. In turn, regulators develop rules both by authoring draft regulations and by eliciting comments from the public about how rules can be practical and enforceable and meet the statutory intent.This combination of separation of duties, inter-branch delegation, and public accountability creates tensions in regulatory rulemaking that encourages the public to both ask for and resist specific requirements from regulators. Some organizations demand specific rules because they are easier to interpret even if they are also more constricting. Other organizations demand vague rules that are easier to tailor to business practicalities even if they increase potential liabilities when regulators disagree with an organization's interpretation of the rules.

In 1993, the Clinton administration issued Executive Order 12866[24] to provide better direction for finding the right blend of regulatory direction and industry flexibility. E.O. 12866 formalized a practice that some executive agencies used to determine whether a rule sufficiently balanced statutory intent with economic feasibility. Risk analysis, it stated, would be used by federal agencies to evaluate the efficacy of regulatory rulemaking. E.O. 12866 led to two standard practices in regulatory rulemaking: it standardized regulatory impact analysis as a macro-economic cost-benefit analysis of proposed rules, and it standardized the inclusion of risk analysis and risk management in each regulation.
This latter innovation permitted – and today permits – a covered entity to determine for themselves how to apply safeguards by evaluating the risks that they pose to themselves and to others, and to determine which safeguards would reasonably address those risks.

C. Recommendation

Because no cybersecurity or privacy regulation will innovate as quickly as innovations and threats, and because no regulation can be more specific than the statute that authorizes regulatory rulemaking, covered entities should understand the purpose of HIPAA's risk analysis[25] and risk management[26] specifications to determine how contemporary risks should be managed using contemporary safeguards. HIPAA's Risk Analysis specification requires that covered entities (and now business associates), "Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered

[23] An Overview of Federal Regulations and the Rulemaking Process (congress.gov)
[24] 12866.pdf (archives.gov)
[25] § 164.308(a)(1)(ii)(A).
[26] § 164.308(a)(1)(ii)(B).

entity."[27] While an organization in 2003 would not consider ransomware, IoMT, or web pixel tools a potential risk, or even in 2016 would they think of ransomware as a confidentiality risk, they would certainly think so today.

In brief, if DHHS OCR updated anything at all regarding the HIPAA Security Rule to meet current information security risks, it would be to help covered entities and business associates understand that risk analysis is how organizations determine whether their safeguards and risks are reasonable and appropriate given the nature of contemporary uses of information and the threats against that information.

V. What is the Best Way to Address the Proliferation of Health Data Outside of the Traditional Insured/Insurer Relationship?

- Our position is that the emergence of new privacy issues is best addressed through standalone privacy legislation.
  - (1) Standalone legislation can be drafted in a simple and straightforward manner. Many have critiqued HIPAA as being overly complex and attempting to reform HIPAA may not achieve the desired goal of fostering clarity around the treatment of sensitive health data.
  - (2) HIPAA does not provide for a private right of action; new legislation could potentially have a mechanism for individuals to sue under the law
  - (3) Standalone legislation can better address emerging technologies and their role in the development, proliferation, and use of health data. (AI, telehealth, etc.).
  - (4) Standalone legislation can better address patient consent
  - (5) If standalone privacy legislation had a federal preemption clause, it may get bipartisan support.

- *What the law may address?*
  - **Patient consent** - *Explicit* consent for sharing of PII to entities not directly involved in healthcare treatment (i.e. for purposes of training artificial intelligence)
    - Clear disclosures about: (1) the purposes in which data is being used; (2) where their data is being stored and for how long; and (3) option to decide whether data is shared in anonymized or identifiable form
  - **Principles of data minimization and destruction** - codifying concept that entity should only collect and retain the least amount of information necessary to accomplish task; data should be destroyed if certain conditions are met
  - **Data anonymization** – address situations in which patient information can used anonymously, setting minimum standards for anonymization, which still require patient consent
  - **Minimum security standards** – may address issues such as encryption, monitoring, and limiting access to sensitive information
  - **Liability for negligent disclosures** – there has been a significant increase in PHI-related data breaches, new law can address liability for negligent disclosures similar to CCPA
  - **Liability for intentional disclosures** – potentially harsher penalties for entities that "intentionally" transmit PHI in violation of the law (i.e., statutory damages)
- *How should law interact with HIPAA?*
  - One option would be to say where HIPAA and new law conflict, new law governs (or, alternatively, whichever law has stricter requirements governs)

[27] § 164.308(a)(1)(ii)(A).

- *How should law interact with state laws?*
  - Should not preempt data disclosure and use laws like CCPA, but may preempt state laws specifically addressing healthcare data