College of Healthcare Information Management Executives

January 24, 2020

Energy and Commerce Committee Staff
Consumer Protection & Commerce Subcommittee Staff
U.S. House of Representatives
2125 Rayburn Office Building
Washington, DC 20515

Dear Energy and Commerce Committee staff:

The College of Healthcare Information Management Executives (CHIME) is pleased to provide feedback for the discussion draft addressing consumer privacy disseminated by the bipartisan committee staff on December 18, 2019.

CHIME is a professional organization that represents more than 3,200 Chief Information Officers (CIOs) and other senior healthcare IT leaders. CHIME enables its members and business partners to collaborate, exchange ideas, develop professionally and advocate for the effective use of information management to improve the health and care in the communities they serve. CHIME members are responsible for the selection and implementation of clinical and business systems that are facilitating healthcare transformation through technology. Our members represent some of the earliest and most prolific adopters of electronic health records (EHRs) and other health IT resources. Our mission is, "To advance and serve healthcare leaders and the industry improving health and care globally through the utilization of knowledge and technology."

CHIME appreciates the opportunity to lend our perspective as the committee seeks to advance critical consumer privacy policies, including those that may impact consumer healthcare data. **From our perspective, all data can be healthcare data, which has generated significant concerns among our members around privacy. Among our members, concerns continue to mount as healthcare data is increasingly exchanged both among and outside non-traditional healthcare settings, and as consumers become active managers of their health information. We are particularly concerned that as more patients share their healthcare data with third parties, that data could be mishandled, including being sold to data aggregators and used to discriminate against consumers in the future**. Given the volume of data in question and the sensitive nature of healthcare data, this is cause for concern.

As Congress continues to consider legislation to address privacy issues, CHIME seeks to ensure future changes to federal privacy laws and regulations are feasible for providers and do not create duplication around existing mandates, which could be costly and operationally burdensome. In addition, we want to ensure any changes protect consumers when their healthcare information is shared with parties outside the traditional healthcare environment. **Below we offer our more detailed feedback on the draft along with our recommendations.**

Definition of "Covered Entities"

Our members have a long-standing commitment and legal obligation to protect and secure patient information with which they have been entrusted pursuant to the Health Insurance Portability &

Accountability Act (HIPAA). Healthcare providers take this responsibility very seriously. Similarly, patients expect and have long trusted their healthcare providers to keep their information private.

The term "covered entity" also has a distinct and well-understood meaning within HIPAA. HIPAA privacy rules have been in place since 2002.[1] The Health Information Technology for Economic and Clinical Health (HITECH) Act, which was included as part of the American Recovery and Reinvestment Act of 2009, also created new requirements around privacy and security for HIPAA-covered entities. Under HITECH the "Meaningful Use" program was created (renamed "Promoting Interoperability" program). Importantly, it created requirements for providers to use electronic health records (EHRs) in certain ways. Included among the program requirements is that providers must perform an annual risk assessment pursuant to HIPAA. Failure to meet this requirement results in significant financial penalties in the form of reduced Medicare reimbursement. This all said, HIPAA is inextricably linked to numerous other federal mandates that carry hefty penalties for non-compliance.

As drafted, this legislation appears to require both HIPAA and non-HIPAA covered entities to comply with the provisions outlined in this draft. **While we appreciate the committee's efforts to impose strong privacy safeguards for consumers, if left unchanged, this legislation could be crippling for healthcare providers.**

Section 17 of the draft defines "covered entities" and gives broad latitude and oversight to the Federal Trade Commission, stating:

> *(A) means any organization, corporation, trust, partnership, estate, cooperative, association, sole proprietorship, unincorporated association, or other entity, over which the Commission has authority pursuant to section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)), that processes covered information;*
> *(B) notwithstanding section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)), common carriers; and*
> *(C) notwithstanding sections 4 and 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 44 and 45(a)(2)), any nonprofit organization, including any organization described in section 501(c) of the Internal Revenue Code of 1986 that is exempt from taxation under section 501(a) of the Internal Revenue Code of 1986.*

HIPAA already requires several protections for patients that would be duplicated under this draft, and if adopted as law, will create significant confusion and duplicative requirements for healthcare providers. These include, but are not limited to: 1) stringent privacy and security requirements, including ones that place strict restrictions on the sharing of patient information; 2) prohibitions around the sale and marketing of patient data;[2] 3) requirements for performing risk assessments;[3] and 4) significant penalties for data breaches.[4] Below are some examples.

Section 3 on Transparency contains a requirement to file an annual submission to the FTC, which contains among many other things:

> *an assessment of the risks posed to individuals as a result of the covered entity's processing of covered information, and a general description of the measures the covered entity has taken or will take to address such risks.*

Section 4 on the Privacy Program also calls covered entities to:

---

[1] https://www.hhs.gov/hipaa/for-professionals/privacy/index.html
[2] 45 CFR §164.508 Uses and disclosures for which an authorization is required.
[3] 45 CFR Appendix A to Subpart C of Part 164
[4] https://www.federalregister.gov/documents/2019/04/30/2019-08530/notification-of-enforcement-discretion-regarding-hipaa-civil-money-penalties

establish and implement reasonable policies, practices, and procedures regarding the processing of covered information—
(1) designed to
(A) comply with applicable privacy laws;
(B) consider the mitigation of privacy risks throughout every stage of the covered entity's products and services, including their design, development, launch, and implementation; and
(C) implement reasonable training and safeguards within the covered entity to promote compliance with all privacy laws applicable to covered information the covered entity processes and mitigate privacy risks;

As noted earlier, both HIPAA and HITECH require healthcare providers (and the Medicare Access and CHIP Reauthorization Act of 2015 (MACRA) for clinicians) to perform a risk assessment annually. Failure to do so risks a provider's Medicare reimbursement and could leave them open to a breach of healthcare data, which carries significant financial penalties and reputational harm. Thus, providers take seriously their obligations to meet these obligations. And, these responsibilities are deeply engrained in the requirements healthcare providers must meet.

CHIME Recommendations:

1. Strong privacy protections for consumers are needed to ensure that third parties and data aggregators are not using data in ways not envisioned by consumers.
2. Given HIPAA covered entities already have long-standing, stringent privacy and security requirements that must be met, they should be carved out of this legislation. Without an exemption, this will create dual requirements for healthcare providers to meet, which will create enormous confusion, significant complexity and unnecessary costs to the healthcare system.
3. Modify the term "covered entities" to avoid confusion within the healthcare industry.

Covered Information

Similar to the concerns expressed above concerning duplication around burdensome mandates, our members are very concerned that the term "covered information" is exceptionally broad when viewed through the lenses of a healthcare provider. If left unchanged and providers have to meet this definition, it will create a scenario where millions of data points will be included and significant tracking processes will have to be put into place. Our members have concluded this could be nearly impossible to implement. While HIPAA is not as granular as what is being proposed, there are nonetheless requirements around what data and under what circumstances it can be released.

CHIME Recommendation: The bill should exempt healthcare providers who already comply with HIPAA and continue allowing healthcare information to be shared by HIPAA-covered entities when it is for "treatment, payment and healthcare operations."[5]

Privacy Responsibilities for Entities Not Covered by HIPAA

While healthcare providers must protect and safeguard patient information, they are also required – when requested by a patient - to share their information with third parties not covered by HIPAA. What is not required by existing law today, however, are any federal privacy and security requirements for the way healthcare data is handled by third party apps. We are therefore pleased the committee is taking seriously the issue of data in ways not envisioned or authorized by consumers.

To provide some more context as to our concerns with third party use of healthcare data, we offer some additional background. The 21st Century Cures Act of 2016 requires healthcare providers to offer patients

[5] 45 CFR §164.506 Uses and disclosures to carry out treatment, payment, or health care operations.

access to their information by way of application programming interfaces (APIs). APIs are a technology widely in use today on smart phones that allow apps to access information from websites (and in the case of healthcare providers, access to the data stored in electronic health records (EHRs)) and display it in useable manners on their phones. This technology is used by many other industries today which consumers routinely use for the purposes of convenience. As an example, a few well understood use cases are a banking apps, airline booking apps and driving direction apps.

While healthcare providers must comply with a patient's request to release their medical information to a third-party app, what is widely misunderstood by patients, and the public at large, is that once a patient requests their information be disclosed to one of these third parties, their information is no longer protected under HIPAA. These third parties may (and in many cases have already) re-disclose and or sell consumer health information to others, including data aggregators. This is eroding consumer trust and there are well-documented instances of this happening today.

The deluge of data that will flow from healthcare provider systems through APIs to third parties will be enormous. We expect a tsunami of data to flow the marketplace, jeopardizing patient / consumer privacy. Once Pandora's box has been opened, there is no way to close the lid. One of our members astutely described his concerns around this very scenario is a recent op-ed, which you can find here.

CHIME Recommendation: CHIME supports policies aimed at ensuring third parties not covered by HIPAA must meet privacy requirements that inform patients and seek consent prior to their information being released or sold.

Definition of Health Information

We understand the committee is very interested in feedback concerning how best to craft the definition of health information (Section 17 on Definitions). As a preliminary matter, as discussed above, healthcare data held by covered entities should be carved out of this bill and thus the definition. We believe this should apply in so far as the data has not yet been requested to be released by a patient to a non-HIPAA covered entity. Once, however, a patient consents to have their data released, we believe this data should fall within the definition of "health information" for the purposes of this bill.

Second, increasingly, all data can be considered health data in light of the fact that the aggregation of enough data points can pinpoint an individual. This becomes especially true once you have GPS location data.

CHIME Recommendation: Treat all healthcare data that has been released by a patient to a third party (as is thus no longer protected by HIPAA) as "health information."

De-identified Data

Section 17 on Definitions includes the definition of "covered information" and the draft specifically excludes de-identified information. There is growing evidence that information can no longer be de-identified. With relative ease, large datasets can elicit the identity of individuals and this is occurring as a result of data shared by consumer via third party apps and GPS location data.[6, 7]

CHIME Recommendation: The committee should consider that de-identified data can now without too much effort be re-identified.

[6] https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html?emc=edit_na_20181210&nl=breaking-news&nlid=42062092ing-news&ref=headline
[7] https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html?emc=edit_na_20181210&nl=breaking-news&nlid=42062092ing-news&ref=headline

Rules

There are instances where the draft calls upon the FTC to promulgate rules. We are concerned that the volume of rules could create significant administrative burdens. There appear to be at least a dozen requirements for regulations contained in the draft. While we appreciate the need for oversight and the committee's commitment to consumer privacy, we believe fewer regulations could be more efficient.

CHIME Recommendation: Consolidate the number of required rulemaking to minimize complexity for the industry and facilitate a more streamlined pathway toward compliance.

Conclusion

We appreciate the opportunity to comment and welcome the chance to help inform the important work being done by Congress. We look forward to continuing to be a trusted stakeholder on protecting consumer privacy as the healthcare sectors continues to adapt to the still nascent opportunities with electronic/digital/virtual healthcare. Should you have any questions about our letter, please contact Mari Savickis, Vice President of Public Policy, at msavickis@chimecentral.org.

Sincerely,

Russell P. Branzell, CHCIO, LCHIME
President and CEO
CHIME

John Kravitz, CHCIO, MHA
Chair, CHIME Board of Trustees
Chief Information Officer
Geisinger Health System