Massachusetts Health Data Consortium

HHS OCR HIPAA Privacy Rule to Support Reproductive Health Care Privacy (HHS-OCR-2023-0006-0001) Comment

This document is submitted by the Massachusetts Health Data Consortium (MHDC) and its Data Governance Collaborative (DGC) in response to the HHS OCR HIPAA Privacy Rule to Support Reproductive Health Care Privacy NPRM (HHS-OCR-2023-0006-0001) posted in the Federal Register on April 17, 2023 and found here: https://www.federalregister.gov/documents/2023/04/17/2023-07517/hipaa-privacy-rule-to-support-reproductive-health-care-privacy

About MHDC

Founded in 1978, MHDC, a not-for-profit corporation, convenes the Massachusetts's health information community in advancing multi-stakeholder health data collaborations. MHDC's members include payers, providers, industry associations, state and federal agencies, technology and services companies, and consumers. The Consortium is the oldest organization of its kind in the country.

MHDC provides a variety of services to its members including educational and networking opportunities, analytics services on both the administrative and clinical side (Spotlight), and data governance and standardization efforts for both clinical and administrative data (the Data Governance Collaborative/DGC and the New England Healthcare Exchange Network, respectively).

About DGC

The DGC is a collaboration between payer and provider organizations convened to discuss, design, and implement data sharing and interoperability among payers, providers, patients/members, and other interested parties who need health data. It is a one stop interoperability resource. The DGC primarily focuses on three areas:

1. Collaboration: Development of common understanding of and specifications for data standards, exchange mechanisms, and what it means to participate in the modern health IT ecosystem
2. Education: helping members understand their regulatory obligations, the data and exchange standards they're expected to use, and modern technology and related processes
3. Innovation: Identification and development of projects and services needed to make modern health data practices and exchange a reality

General Comments

This section comments on the general approach taken by HHS OCR in their posted proposal or comments on items that cross multiple sections of the proposed rule

NCVHS Response to NPRM on June 14, 2023 Full Committee meeting

NOTE: NCVHS later clarified in a dedicated afternoon session of the same committee meeting that the recommendation outlined below was not their intent. However, some of our response may still be applicable to the comments they do intend to make in terms of the scope of attestation requirements and may still be informative to OCR. Given the timing of the comment deadline, we have decided to leave the comment in place rather than try to determine which parts, if any, still apply to NCVHS' corrected indication of their intent or may be more generally useful.

During the overview of its recommendations related to this NPRM given during the 10am hour of the NCVHS Full Committee meeting held on June 14, NCVHS noted it intends to recommend that all requests for PHI by all parties require an attestation that any received data will not be used for the proscribed activities as outlined in this NPRM.

While we appreciate the intent behind this request, we are concerned that such a requirement would delay and/or prevent automated data exchange using FHIR APIs as outlined in existing HHS proposed and final rules from CMS, ONC, and others. Among other things, these rules require the exchange of USCDI v1 data via FHIR APIs between various combinations of payers, providers, and patients (as represented by third party applications and other such vehicles).

If such a recommendation is adopted and absorbed into a final rule, we urge OCR to consider how this requirement could be met without impeding existing regulated exchanges or industry innovations using more extensive data exchange via FHIR APIs.

For example, one possible approach would be to require exchange of a specific FHIR resource representing the required attestation to happen before more verbose API calls follow. This approach is, in theory, straightforward and fairly lightweight, but incorporating it into regulation would likely require an industry Standards Development Organization to take up the work of developing this resource/profile, setting the rules for its use, and otherwise defining related data and workflows. This would then need to be tested, voted upon, and go through the formal standards adoption process before it could then be adopted into other rulemaking including a final version of this rule and related CMS/ONC regulations such as adoption into health IT certification requirements or use by payers in already required exchanges of PHI. Other approaches may require similar development and adoption efforts.

In addition, a “60 day after publication” effective date with a 180 day compliance date would likely not be sufficient to implement an attestation process for FHIR APIs.

Effective Date vs Compliance Date

We note the rule includes language around an effective date (60 days after publication) vs compliance date (180 days after publication). It is not clear precisely what each of these terms mean in terms of expectations of implementation, enforcement, and penalties.

Other entities participating in enforcement

NCVHS is also recommending working with other agencies such as the FTC to provide consistent enforcement and rules around the use and sharing of reproductive health data. We note that the FTC does not have authority over non-profit organizations so this would not be as all-reaching as perhaps intended by NCVHS.

TEFCA

NHCVS recommends that attestation of compliance with reproductive health data use be part of the TEFCA requirements that all QHINs, participants, and subparticipants must follow. We approve of this suggestion.

Interoperability and Information Blocking

NCVHS indicates that additional changes and rules related to reproductive health privacy should be explicitly addressed in terms of interoperability and information blocking rules as set by CMS and ONC without providing any specific suggestions. We concur that consideration of these topics be part of the overall reproductive health privacy conversation, but also caution that this be done by or in consultation with experts on those rules and on pending/upcoming regulations so as to avoid conflicting requirements.

Reproductive Health Care and Retail Purchases

The proposed definition of reproductive health care includes services and supplies provided by non-healthcare entities including “care, services, or supplies furnished by other persons and non-prescription supplies purchased in connection with an individual's reproductive health”. These activities provided outside of the traditional healthcare provider ecosystem would typically occur outside of the mandates of HIPAA and not be considered under HIPAA privacy rules.

It is unclear that HIPAA has the authority to extend beyond its traditional boundaries, but putting that aside for the moment, it seems like the intent of this rule is to apply the privacy requirements and attestation rules to entities that fulfill retail sales of over the counter supplies related to reproductive care in any way. We feel any final rule should clarify this intent and, if necessary, outline exactly how the new privacy rules would apply to retail outlets and non-traditional service providers outside of the standard HIPAA actors.

Penalties when HIPAA and Court Orders Disagree

We note that the NPRM specifically address the case where a court order may direct someone to disclose data that the new HIPAA proposals would prohibit them from disclosing. The proposed rule indicates:

“It would also prohibit the disclosure of PHI for a law enforcement investigation of a health clinic for providing reproductive health care that is lawful under the circumstances in which it is provided, even in response to a court order, such as a search warrant.

Such disclosure, despite the court order, would be a violation of the Privacy Rule and would subject the regulated entity to a potential OCR investigation and civil money penalty. Additionally, if a regulated entity chose to comply with the court order in the example above, there would be a presumption that a breach of unsecured PHI had occurred because there was a disclosure of PHI in a manner not permitted under the Privacy Rule which compromises the privacy of the PHI. Thus, breach notification would be required unless the entity could demonstrate that there was a low probability that the PHI had been compromised.

Where an entity determines that a breach has occurred, the entity would need to provide notification to the affected individual(s), the Secretary, and, when applicable, the media.”

We note that this puts the entity receiving a court order in an untenable position. The penalties for ignoring a court order are, in general, significantly more severe than those for violating HIPAA, up to and including potential incarceration of individuals involved. While the entity could push back on the court order based on their legal obligations to follow HIPAA, this is at best costly and at worst may be unsuccessful and put the entity in the position of either violating HIPAA or going to jail/facing other court injunctions.

Addressing Rapidly Changing Laws

The proposed rule indicates the requirements of non-disclosure of information is tied to the current legality of the actions generating the reproductive health data. We note that local and state laws in this area are changing rapidly and what is legal one day may be illegal the next. We suggest a grace period of 30 or 60 days to adjust to changing laws might be appropriate to allow changes to be properly absorbed and acted upon by all relevant entities.

Belief that Attestation Was False

The proposed rule indicates that a regulated entity should stop disclosure of PHI if they have reason to believe that the attestation received was materially false and related data is being used or disclosed for a prohibited purpose. We note that some additional guidance on the documentation required to back up this decision and any requirements around allowing the requesting entity to dispute this decision/how that dispute should be adjudicated seems warranted to allow for a standardized approach to this situation.

Response to Specific Questions

This section will list specific questions asked about the attestations and allowed use of reproductive health data in the proposal and our responses to them.

Whether requesters of PHI should be required to name the individuals whose PHI they are requesting, or if describing a class of individuals whose PHI is requested is sufficient. Please explain how the Department can further protect the privacy of individuals from requests for large amounts of PHI ostensibly sought for a non-prohibited purpose if requesters of PHI are permitted to

describe a class of individuals whose PHI is requested.

We note that patient matching issues may come into play if the only requirement is to name the individual patients covered by a request. We strongly suggest that sufficient identifying information to ensure that the proper patients and only the proper patients are included in any data request be required.

Whether a model attestation would be useful for regulated entities/Whether the Department should require a particular attestation format, rather than providing a model attestation

We believe one or more sample attestations would be useful. We do not support requiring the use of specific attestation text as it may be difficult to craft one that would apply to all situations, but providing some guidance and samples around the type of information to include and how to make a valid request that passes muster would be appropriate.

Whether the Department should require the attestation to include a signed declaration made under penalty of perjury that the requester is not making the request for a purpose prohibited by this proposal and any ramifications, positive or negative, of such a requirement.

Given that these attestations are designed to be used in cases of legal and administrative proceedings, it seems reasonable to make the attestation a binding document with some real penalty for falsification. For legal and formal administrative proceedings, penalty of perjury seems a common standard. We would accept that in other cases as well or be open to alternatives; we do not know If the meaning, enforcement mechanisms, and consequences of penalty of perjury is as clear for other potential use cases.