Business Group on Health

June 16, 2023

U.S. Department of Health and Human Services
Office of Civil Rights
Via: regulations.gov submission

Re: Business Group on Health Comments on HIPAA and Reproductive Health Care Privacy NPRM – Docket ID: HHS-OCR-0945-AA20 (RIN Number 0945–AA20)

To whom it may concern:

Business Group on Health appreciates the opportunity to comment on the NPRM listed above. We appreciate the Office of Civil Rights' (OCR) attention and effort to update HIPAA and help ensure group health plans and other covered entities have reliable, pragmatic guidance regarding the handling of protected health information.

Business Group on Health represents a network of more than 440 of today's largest and most progressive employers and industry partners including 72 Fortune 100 companies, providing health coverage for 60 million workers, retirees and their families in 200 countries. Business Group members – innovative employer plan sponsors – are leading the way and encouraging others by providing strong health plan offerings, adopting alternative payment models, managing the total cost of care, promoting health equity, furthering population health, and keeping people well.

In general, Business Group on Health's comments here will focus on the practical implementation of additional protections and prohibitions from use and disclosure that OCR proposes to apply to reproductive health care information. We wish to help ensure that health plans, other covered entities, business associates, and others to which these new requirements would apply (collectively "covered entities") are able to reasonably comply, maintain privacy, and balance other legitimate interests.

I. The proposed attestation requirement should apply to all exceptions under 45 CFR 164.512 regardless of the intent of the request or nature of the information requested.

20 F Street, NW
Suite 200
Washington, DC 20001

202-558-3000
info@businessgrouphealth.org

Visit us at:
www. businessgrouphealth.org

We are concerned that covered entities will not have the ability, information, resources, or capacity to review or dispute the asserted standard or characterization of a request based on any of the exceptions under 45 CFR 164.512 as they would pertain to the new prohibitions. We believe broad application of the attestation requirement to all of these exceptions presents no material burden to any requestor whose purpose is not prohibited regardless of the applicable standard identified. The requestor is in the best position to confirm both their legal basis for the request and whether the request is for a prohibited purpose and should bear the burden of such determination rather than the covered entity. Thus, the attestation requirement should apply to all requests for use or disclosure of information under the exceptions set forth in 45 CFR 164.512.

Additionally, as discussed in more detail below, it is unworkable to assess and assure that protected health information (PHI) does not contain information "potentially related" to reproductive health care. Thus, the attestation should apply without regard to the intended or actual terms of such request as it relates directly or indirectly to reproductive health care information and instead apply to all requests under §164.512.

II. The attestation should require the requestor to declare, certify, verify (or other appropriate term) under penalty of perjury under the laws of the United States of America that the contents, assertions, and substance of attestation and the representations therein are true and correct.

As referenced above, the requesting party is best situated to determine the legal basis for the request as well as to make representations regarding the intentions associated with the use and disclosure of PHI. This heightened standard around the request would enable the covered entity to reasonably rely in good faith on the substance of the attestation without further investigation, delay, cost, burden, or dispute. A requestor acting in good faith and making a compliant request that is not for a prohibited purpose should have minimal to no concern providing this assurance.

III. Covered entities should be considered in compliance with the new rules if they rely in good faith on an attestation which appears on its face to satisfy the requirements.

Covered entities generally will not be in a position to heavily investigate or dispute requests under these new restrictions and should not be required to do so. If presented with an apparently compliant request that is supported by a facially complete and satisfactory attestation, the covered entity's good faith reliance in providing the requested information is justified. Relatedly, the "actual knowledge" and "objectively unreasonable"

provision proposed at §164.509(b)(2)(iv) & (v) should be struck or revised and clarified to conform to a good faith reliance standard. At minimum, it is unclear what would constitute "actual knowledge" or when a covered entity's belief is "objectively unreasonable," among other questions raised by these proposed subparagraphs.

IV. Failure to provide a valid attestation should bar use or disclosure of any PHI under the related request, not just bar the portion of such PHI that is "potentially related to reproductive health care".

Under §164.509(a) as proposed, it appears that a covered entity may be expected to parse through PHI and remove or redact any that is or could be "potentially related" to reproductive health care. This would be an unworkable expectation and should be revised. To start, the determination of whether information is "potentially related" to reproductive health care is vague, evolving, and indeterminable. There may be certain items and services in the PHI that could easily be associated with such care (e.g., items with certain billing codes) but for other information it is not so clear. There may be instances of apparently "unrelated" PHI from which inferences and correlations may be drawn that imply that reproductive health care was sought or received. A covered entity cannot reasonably be expected to assess, predict, and prevent any and all indirect, attenuated, or correlative information that may be "potentially related" from being provided.

Furthermore, certain data and information storage systems may not be set up to parse through PHI efficiently and to remove or redact "potentially related" information without manual interventions or extraordinary system changes. This would be extremely burdensome and costly for covered entities to undertake, while still leaving uncertainty about the relatedness of the information.

To alleviate these concerns, the covered entity should not provide any information in response to a request that fails to provide a valid attestation or otherwise meet all requirements. This would not preclude the requestor from submitting a new request that satisfies all requirements but would provide certainty and efficiency for covered entities to handle requests that do not meet the standards.

V. Additional comments, requests, and recommendations.

- §164.502(a)(5)(iii)(C) sub (1), (2), and (3) – should all include consideration of circumstances where care is sought or expected to be provided but then is not actually provided, yet some PHI regarding the seeking or consideration of care may exist. This appears potentially to be addressed by substituting "sought, provided,

or expected to be provided" for the word "provided" in each numbered sub-paragraph, or by making a similar revision.

- §164.502(a)(5)(iii)(D) *Rule of Construction* – seems to contain modifiers that raise uncertainty regarding the application of the rule. OCR should consider revisions as follows:

  > Nothing in this section shall be construed to prohibit a use or disclosure of protected health information otherwise permitted by this subpart unless such use or disclosure is ~~primarily~~ for the purpose of investigating or imposing liability on any person for ~~the mere act of~~ seeking, obtaining, providing, or facilitating reproductive health care.

- §164.509(c)(1)(v) – The signature requirement should specify that the "person" must be a natural person that is individually identifiable in order to effectuate the penalty of perjury standard. "Person" otherwise appears to imply that the attestation could be signed in a corporate name (e.g.) alone without individually identifiable attribution for reliance and any applicable enforcement.

- Amend the attestation requirements to include that the requestor represent and guarantee that they will not further use or disclose the PHI for a non-permitted purpose and that the requested information is the minimum necessary for the purpose of the use or disclosure.

- Provide sample attestation language/forms with the revisions suggested herein and permit covered entities to combine the attestation with new or existing documents rather than as a stand-alone document as proposed.

- Requests by an individual for their own information and/or appropriately authorized by an individual should not be subject to review and/or denial by the covered entity under this rule. We are concerned that subjecting individually directed/authorized requests to new scrutiny under this rule may have an adverse effect on an individual's ability and desire to seek information when they otherwise would or should for their own health-related or other personal reasons. Additionally, such review may be unduly burdensome on covered entities to second guess these requests to determine the underlying purpose or impetus for individual/authorized requests.

- Adopt a broad, non-exhaustive definition of "reproductive health care" that includes related items, services, and programs such as, but not limited to, prescription drugs and travel benefits.

- Provide clarity and assurance to covered entities that HIPAA's preemptive effect on state laws applies to circumstances where HIPAA would prohibit use and disclosure of any PHI regardless of whether a state law directly or indirectly would require such disclosure.

- With respect to implementation – provide ample time for covered entities to establish processes and systems to comply with the rules. Adopt a non-enforcement policy for covered entities and business associates acting in good faith to implement the rules and provide that the full preemptive effect on state laws shall apply during such period and otherwise under HIPAA.

- Provide that the covered entity shall not be liable, non-compliant, or considered to have violated HIPAA where it acts in good faith based on a facially valid attestation and permissibly discloses PHI in accordance with these rules, but the requestor/recipient uses or discloses any or all of the PHI in a manner or purpose that would otherwise be prohibited. This should also apply to subsequent uses and disclosures once the PHI leaves the control of the covered entity, e.g., if the requestor/recipient further discloses the information to a third-party which uses it for a prohibited purpose.

- Provide permissive sample language and examples for HIPAA Notice of Privacy Practices updates.

Thank you for your consideration. We would welcome the opportunity to discuss these comments or any other matters impacting employer plan sponsors. Please feel free to contact me (kelsay@businessgrouphealth.org) or Garrett Hohimer, Vice President, Policy and Advocacy (hohimer@businessgrouphealth.org) to discuss further.

Sincerely,

Ellen Kelsay
President and CEO