IPMPC
International Pharmaceutical & Medical Device Privacy Consortium

August 8, 2023

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW, Suite CC–5610 (Annex H)
Washington, DC 20580

Re: Public Comment on the Health Breach Notification Rule, Project No. P205405

Dear Federal Trade Commission:

The International Pharmaceutical & Medical Device Privacy Consortium ("IPMPC") welcomes the opportunity to provide comments on the Commission's proposed regulations revising the Health Breach Notification Rule ("HBNR").

The IPMPC is comprised of chief privacy officers and data privacy and security professionals from a number of global pharmaceutical and medical device manufacturers. The IPMPC is the leading voice in the pharmaceutical and medical device industry to advance innovative privacy solutions to protect patients, enhance healthcare, and support business enablement.[1]

Protecting consumers' electronic personal health records is critical for fortifying individuals' privacy in an increasingly digitized world. To increase transparency and incentivize entities to better secure consumer health data, the Federal Trade Commission (FTC) adopted the Health Breach Notification Rule (HBNR) in 2009, creating a system where consumers are notified when a breach of unsecured electronic health data has occurred. However, technology has changed dramatically since the HBNR was finalized fourteen years ago. Therefore, the FTC's proposed updates are a welcome refresh of the HBNR.

In this Public Comment, the IPMPC seeks to raise two issues for the FTC's consideration as the FTC finalizes its proposed regulations revising the HBNR: (1) the IPMPC requests the FTC include an exemption for the use of personal health records in clinical research, and (2) the IPMPC further requests the FTC clarify the application of the HBNR to disclosures permitted without a patient's authorization under HIPAA.

A. The IPMPC requests the FTC include an exemption for the use of personal health records in clinical research.

[1] More information about the IPMPC is available at https://www.ipmpc.org. These comments reflect the position of the IPMPC as an organization and should not be construed as the positions of any individual member.

Clinical research is vital for medical discovery and innovation. In recent years, clinical researchers have turned to mobile applications and online platforms to ensure trials are accessible, efficient, and diverse.[2] The IPMPC believes that failing to include a specific exemption for the use of personal health records in clinical research will lead to confusion over whether the use of such records is appropriate or permitted in the research context, and will eventually result in a chilling effect whereby researchers are deterred from using mobile applications and online platforms to facilitate research. Therefore, the IPMPC respectfully requests the FTC adopt exemption language for clinical research into the HBNR proposed rulemaking.

First, the IPMPC would like to draw attention to the fact that personal health records used in connection with clinical research should be explicitly exempt from the HBNR proposed rulemaking because they do not fall under the HBNR's definition of a "personal health record" (PHR). Under the proposed rulemaking, PHR is defined as "an electronic record of identifiable health information on an individual that has the technical capacity to draw information from multiple sources and that is managed, shared, and *controlled by or primarily for the individual*."[3] In the context of clinical research, these records are *not* managed, shared, and controlled by or primarily for the individual. Rather, the information is collected for and controlled by research sponsors, for research purposes. Despite this fundamental distinction, the IPMPC recognizes that the research use case sits in a gray area, given that many of the tools used in the research context are indistinguishable from consumer-facing PHRs that fall within the FTC's definition. The lack of specific FTC guidance on the use of such tools in the research context has led to confusion and delays in clinical research settings, as researchers often must address compliance with HBNR requirements alongside other disclosure, notice, and consent requirements set forth by the Food and Drug Administration (FDA), Institutional Review Boards (IRBs), and other regulatory bodies responsible for overseeing clinical research. Therefore, the IPMPC requests the FTC include a clear exemption from HBNR requirements for PHR-like tools used in the clinical research context .

Second, the IPMPC notes that there is precedent for including a specific clinical research exemption, as seen in several states' data privacy laws. In the past decade, various states have enacted consumer data privacy legislation in response to a rise in technology and personal data collection.[4] Some states have adopted language rendering certain information—often health-related—exempt. Although PHR-like tools used in clinical research do not qualify as PHRs under the HBNR as described above, the IPMPC asks for clarity in the proposed rulemaking in the form of a specific exemption for personal health data collected in clinical research settings, in line with

---

[2] See, e.g., https://news.cancerresearchuk.org/2022/11/28/first-of-its-kind-app-for-patients-on-clinical-trials-being-piloted-by-cancer-research-uk/ for a mobile app providing appointment reminders, patient diaries, and access to trial information for a cancer research trial. See also https://www.jmir.org/2016/12/e330/ for a clinical study testing mobile apps for individuals with depression, and https://www.sprim.com/post/3-ways-mobile-clinical-trials-help-clinical-researchers-improve-diversity/ for more information about how mobile clinical trials increase accessibly and diversity.

[3] See the FTC's proposed rulemaking in the Federal Register, under ¶ II.4: https://www.federalregister.gov/documents/2023/06/09/2023-12148/health-breach-notification-rule#citation-57-p37826 [emphasis added].

[4] California was the first state to pass modern consumer privacy laws with the California Consumer Privacy Act in 2018, seen here: https://oag.ca.gov/privacy/ccpa. Currently, nine states have passed comprehensive consumer data privacy laws, and at minimum sixteen states have introduced privacy bills. More detailed information can be located here: https://pro.bloomberglaw.com/brief/state-privacy-legislation-tracker/.

various state laws. Specifically, the IPMPC proposes that the FTC adopt language similar to the language seen in Virginia, which clearly exempts clinical research:

> § 59.1-576. (Effective January 1, 2023) Scope; exemptions …
>
> C. The following information and data is exempt from this chapter:
>
> 1. Protected health information under HIPAA;
>
> 2. Health records for purposes of Title 32.1;
>
> 3. Patient identifying information for purposes of 42 U.S.C. § 290dd-2;
>
> 4. Identifiable private information for purposes of the federal policy for the protection of human subjects under 45 C.F.R. Part 46; *identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines* issued by The International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use*; the protection of human subjects* under 21 C.F.R. Parts 6, 50, and 56, or *personal data used or shared in research conducted* in accordance with the requirements set forth in this chapter, or other research conducted in accordance with applicable law ….[5] [emphasis added]

Finally, the IPMPC requests a specific exemption for PHR-like tools used in the clinical research context because clinical research falls under the jurisdiction of the FDA.[6] The FDA regulates the welfare of human research subjects, and is responsible for ensuring that IRBs also "protect the rights and welfare of human subjects involved in [clinical] investigations."[7] The FDA requires IRBs to review potential clinical studies to ensure they satisfy detailed requirements designed to protect patients, including that clinical studies adequately protect patient privacy and maintain the confidentiality of data collected in the context of clinical research.[8] Without an exemption for clinical research, research with electronic aspects will require oversight from both the FTC and the FDA. The IPMPC believes that such additional oversight is redundant and will result in greater administrative burden for researchers, and for the FTC as the regulatory body. To reduce the regulatory burden associated with clinical research, the IPMPC respectfully requests the FTC incorporate clear language exempting PHR-like tools, web platforms, and mobile health applications used in the context of clinical research from the HBNR.

B. The IPMPC further requests the FTC clarify the application of the HBNR to disclosures permitted without a patient's authorization under HIPAA.

---

[5] § 59.1-576 is available here: https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/. Virginia is not the only state to include this exemption—Colorado, Indiana, Iowa, and more have also followed suit in protecting the information collected in clinical research. See e,g.,https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf; https://iga.in.gov/pdf-documents/123/2023/senate/bills/SB0005/SB0005.05.ENRH.pdf; https://www.legis.iowa.gov/docs/publications/LGE/90/SF262.pdf.

[6] For more information, please visit the Food and Drug Administration website: https://www.fda.gov/patients/clinical-trials-what-patients-need-know/basics-about-clinical-trials.

[7] See 21 CFR Part 56, found here: https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-56.

[8] See § 56.111 Criteria for IRB approval

The IPMPC recognizes that the HBNR is designed to address consumer protection concerns related to health data held by entities that are not "covered entities" or "business associates" for HIPAA purposes. However, by treating any disclosure of information as a "breach" in the absence of patient consent, the FTC risks extending consent and authorization requirements to situations in which HHS elected to forgo such requirements to improve patient treatment outcomes and ensure appropriate payment for health care. The IPMPC urges the FTC to adopt exemptions from its consent requirements that mirror those found in the Privacy Rule to avoid creating barriers to the flow of information required to provide treatment and ensure payment.

Covered entities may disclose information to IPMPC member companies for a variety of purposes. In some cases, a patient signs a HIPAA authorization, but in others the disclosure is made pursuant to exemptions to the authorization requirements under HIPAA. Requiring the recipient organization to obtain a patient consent before it could, for example, disclose the same information back to the patient's doctor or to the patient's insurer risks creating delay in providing beneficial patient support, discount, or rebate programs. These delays put therapy initiation at risk and can have a direct impact on patient health and medication cost.

For example, HHS has long recognized that HIPAA permits covered entities to make disclosures to other "non-covered-entity" health care providers. These can include, for example, medical device manufacturers who are assisting a surgeon to implant a prosthetic in a patient.[9] Such "non-covered entity" health care providers are not currently exempt from the HBNR.[10] Failure to include a relevant exemption for such entities could lead to a situation where a medical device company providing care to a patient would be prohibited from disclosing information it had properly received from a physician back to the same physician unless it first obtained a patient authorization. This result would defeat the purpose of the exemptions to the patient authorization requirements for these disclosures under HIPAA and prevent "non-covered-entity" health care providers from coordinating around patient care with covered entities.

Likewise, the Privacy Rule permits, without a patient's authorization, a variety of disclosures for recognized public health purposes.[11] In particular, the Privacy Rule permits disclosures of PHI to pharmaceutical, biologic, and medical device manufacturers who are responsible for ensuring the safety and quality of their products and making certain reports to the FDA.[12] Again, the HBNR's current focus on treating all unauthorized disclosures as a reportable "breach" raises a potential concern. If the FTC were to take the position that these reports from providers could not be supplemented with other patient information held by a manufacturer without the patient's authorization (or worse, could not be disclosed to the FDA without authorization), manufacturers of regulated products would face barriers to accomplishing their regulatory obligations to improve patient safety and ensure the quality of regulated products.

Accordingly, the IPMPC asks that the FTC adopt a modification to its definition of "breach" under the HBNR that accounts for the disclosures permitted without a patient's authorization under

[9] 490-When may a provider disclose protected health information to a medical device company representative | HHS.gov.
[10] See, generally, 16 CFR 318.1.
[11] 45 CFR 164.512(b)
[12] 45 CFR 164.512(b)(1)(iii)

HIPAA. For example, the FTC could add the following underlined text to 16 CFR 318.2(a): "Breach of security means, with respect to unsecured PHR identifiable health information of an individual in a personal health record, acquisition of such information without the authorization of the individual. Unauthorized acquisition will be presumed to include unauthorized access to unsecured PHR identifiable health information unless the vendor of personal health records, PHR related entity, or third party service provider that experienced the breach has reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information. However, a disclosure of information made by a vendor of personal health records, PHR related entity, or third party service provider will not be considered a "breach of security" if that disclosure (i) would be permitted without an authorization if that vendor of personal health records, PHR related entity, or third party service provider were a HIPAA-covered entity or engaged in activities as a business associate of a HIPAA-covered entity, (ii) is made to a HIPAA-covered entity or an entity acting as a business associate of a HIPAA-covered entity for the purposes related to treatment or payment (as those terms are defined under the Health Insurance Portability and Accountability Act, Public Law 104-191, 110 Stat. 1936, as defined in 45 CFR 164.502) or (iii) is required for compliance with a legal obligation arising under federal, state, or local law or is made to a government authority with responsibility for oversight of the vendor of personal health records, PHR related entity, or third party service provider."

Conclusion

The IPMPC appreciates the opportunity to comment on the proposed HBNR rulemaking. Thank you for considering our recommendations to request the FTC provide an exemption for the use of personal health records in clinical research and to clarify the application of the HBNR to disclosures permitted without a patient's authorization under HIPAA.

Sincerely,

Reed Abrahamson
IPMPC Secretariat
1500 K Street NW, Suite 1100
Washington, DC 20005
Reed.Abrahamson@faegredrinker.com
(202) 230-5672