August 8, 2023

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

Re: Health Breach Notification Rule, Project No. P205405

Submitted electronically at: https://www.regulations.gov

Dear Secretary Tabor:

As nursing stakeholders, the Alliance for Nursing Informatics (ANI) is pleased to offer comments on the **Health Breach Notification Rule.**

The Alliance for Nursing Informatics (ANI), cosponsored by AMIA and HIMSS, advances nursing informatics leadership, practice, education, policy, and research through a unified voice of nursing informatics organizations. We transform health and healthcare through nursing informatics and innovation. ANI is a collaboration of organizations representing more than 25,000 nurse informaticists and bringing together 29 distinct nursing informatics groups globally. ANI crosses academia, practice, industry, and nursing specialty boundaries and collaborates with the more than 4 million nurses in practice today.

We support the FTC's efforts to clarify the scope and definitions in the Health Breach Notification Rule (the "HBN Rule"). Our practice and research as nurse informaticists demonstrates the need for strong and detailed policies guiding digital health oversight. Across reviews of mobile applications for heart failure,[1] atrial fibrillation,[2] cardiac rehabilitation,[3] depression,[4] and COVID-19,[5] evidence demonstrates

[1] Masterson Creber RM, Maurer MS, Reading M, Hiraldo G, Hickey KT, Iribarren S. Review and Analysis of Existing Mobile Phone Apps to Support Heart Failure Symptom Monitoring and Self-Care Management Using the Mobile Application Rating Scale (MARS). *JMIR Mhealth Uhealth*. 2016;4(2):e74.
[2] Turchioe MR, Jimenez V, Isaac S, Alshalabi M, Slotwiner D, Creber RM. Review of mobile applications for the detection and management of atrial fibrillation. *Heart Rhythm O2*. 2020;1(1):35-43.
[3] Meddar JM, Ponnapalli A, Azhar R, Turchioe MR, Duran AT, Creber RM. A Structured Review of Commercially Available Cardiac Rehabilitation mHealth Applications Using the Mobile Application Rating Scale. *J Cardiopulm Rehabil Prev*. 2022;42(3):141-147.
[4] Myers A, Chesebrough L, Hu R, Turchioe MR, Pathak J, Creber RM. Evaluating Commercially Available Mobile Apps for Depression Self-Management. *AMIA Annu Symp Proc*. 2020;2020:906-914.
[5] Schmeelk S, Davis A, Li Q, et al. Monitoring Symptoms of COVID-19: Review of Mobile Apps. *JMIR Mhealth Uhealth*. 2022;10(6):e36065.

that including a privacy policy can be highly variable and may be as low as 50-75%. This evidence underscores the risks to consumers beyond unanticipated exposure of personal health information and the importance of the HBN Rule.

In support of this goal, we propose the following to add clarity:

1. **Clarify the notification requirements for transferring personal health information (PHI) across companies to which consumers did not initially consent.** Recognizing that an unintentional breach differs from intentional disclosure, there is an opportunity to clarify whether and how consumers producing health data should be notified when Personal Health Information (PHI) is transferred between companies due to mergers and acquisitions. For example, the private equity firm Blackstone acquired Ancestry.com in 2020 and acquired the genetic data gained through Ancestry's at-home DNA kit.[6] This method of acquiring data raises ethical questions around the consumer's autonomy, who has little control over which secondary parties acquire their data, and the potential injustices of personal health data used for commercial purposes in ways that may harm or disadvantage the consumer. We highlight the opportunity to align with the Office for Human Research Protections (OHRP) existing guidelines that protect the secondary use of health data in biomedical research contexts.[7] Information about whether and how secondary data sharing may occur should be included in consumers' initial end-user license agreements. Further, unanticipated data sharing should require new consumer consent.

2. **Require clear and accessible language in end-user license agreements/privacy policies and breach notifications in digital health technologies**. There are no requirements regarding the reading level or comprehensibility of end-user license agreements or breach notifications. Consumers often need more clarity about the precise details for which they consent. These agreements/policies are usually cumbersome and time-consuming to read. A recent study estimated that the average Internet user would need 76 working days to read all agreements they encounter thoroughly.[8] Unnecessary complexity has the potential to exacerbate disparities for lower literacy populations. It may generally result in a need for more of clarity among consumers about how their health data is used and their legal rights to govern the use, re-use and exchange of PHI.

3. **Broaden the definition and requirements for custodianship and responsible conduct using PHI.** We applaud the efforts to broaden the definitions of PHR-related entities and agree with the FTC's notion that these entities should be defined less by how they self-identify and more by the actual or potential opportunity for them to collect, manage, or share health data. We highlight

[6] Blackstone to acquire ancestry®, leading online family history business, for $4.7 billion. Blackstone. Published August 5, 2020. Accessed July 28, 2023. https://www.blackstone.com/news/press/blackstone-to-acquire-ancestry-leading-online-family-history-business-for-4-7-billion/

[7] Office for Human Research Protections (OHRP). Coded Private Information or Biospecimens Used in research. HHS.gov. Published September 19, 2017. Accessed July 28, 2023. https://www.hhs.gov/ohrp/coded-private-information-or-biospecimens-used-research.html

[8] McDonald AM, Reeder RW, Kelley PG, Cranor LF. A Comparative Study of Online Privacy Policies and Formats. In: *Privacy Enhancing Technologies*. Springer Berlin Heidelberg; 2009:37-55.

recent examples of large language model-driven tools including health-focused Chatbots and even non-health-focused entities like ChatGPT, which may be used for health-related purposes, as support for a broad definition.[9,10] Therefore, we advocate for training in the responsible use of PHI among any entity that is a custodian of PHI regardless of self-identification. Accordingly, the FTC might consider HIPAA training – currently a common requirement for any individual or entity working with PHI – for those working at these entities and working with consumers' health data.

4. **Clarify how monitoring and enforcement of the data breach regulations are conducted.** It is unclear whether there is a responsibility for self-reporting or how the FTC becomes aware of data breaches. However, recent examples of identified breaches (e.g., GoodRx)[11] in the notice suggest these mechanisms are in place.

5. **Clarify whether and how the FTC is attempting to align with other agencies involved in regulating digital health tools, primarily the FDA.** The FTC appears to be taking a broader stance than the FDA on regulating the privacy of data collected by digital health tools. This stance could create confusion among developers and business owners if there is overlapping or conflicting regulation. FTC and FDA should collaborate to develop a consensus on digital health tool and PHI definitions, then seek opportunities to clarify regulatory requirements and establish policy precedence.

6. **Provide a definitions page for definitions borrowed from other organizations.** Given the importance of these definitions in clarifying the scope of the HBN Rule, a definitions page will aid the reader in being able to easily understand the guiding definitions referred to in the document without needing to research each meaning.

In conclusion, we support the FTC's efforts to clarify the scope and definitions of the HBN Rule. Thank you for the opportunity to comment.

Sincerely,

Susan C. Hull

Susan Hull, MSN, RN-BC, NEA-BC, FAMIA
ANI Co-chair

Nancy Beale, Ph.D., RN-BC
ANI Co-chair

[9] Sallam M. ChatGPT Utility in Healthcare Education, Research, and Practice: Systematic Review on the Promising Perspectives and Valid Concerns. *Healthcare (Basel)*. 2023;11(6). doi:10.3390/healthcare11060887

[10] Van Bulck L, Moons P. What if your patient switches from Dr. Google to Dr. ChatGPT? A vignette-based survey of the trustworthiness, value and danger of ChatGPT-generated responses to health questions. *Eur J Cardiovasc Nurs*. Published online April 24, 2023. doi:10.1093/eurjcn/zvad038

[11] Fair, L. (2023, February 1). First FTC Health Breach Notification Rule case addresses GoodRx's not-so-good privacy practices*. Federal Trade Commission.* https://www.ftc.gov/business-guidance/blog/2023/02/first-ftc-health-breach-notification-rule-case-addresses-goodrxs-not-so-good-privacy-practices