September 28, 2021

The Honorable Maria Cantwell
Chair
Senate Committee on
Commerce, Science & Transportation
Washington, D.C. 20510

The Honorable Roger Wicker
Ranking Member
Senate Committee on
Commerce, Science & Transportation
Washington, D.C. 20510

Dear Chair Cantwell and Ranking Member Wicker:

On behalf of the Confidentiality Coalition, we thank you for holding a hearing on, "Protecting Consumer Privacy."

The Confidentiality Coalition is composed of a broad group of hospitals, medical teaching colleges, health plans, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health product distributors, pharmacies, pharmacy benefit managers, health information and research organizations, patient groups, and others founded to advance effective patient confidentiality protections. The Coalition's mission is to advocate policies and practices that safeguard the privacy of patients and healthcare consumers while, at the same time, enabling the essential flow of patient information that is critical to the timely and effective delivery of healthcare, improvements in quality and safety, and the development of new lifesaving and life-enhancing medical interventions.

Accessing and sharing health data allows providers to deliver quality care and enables patients to become more engaged in their health decisions. While the Health Insurance Portability and Accountability Act (HIPAA) safeguards a specific subset of "protected health information" (PHI) held by specified types of healthcare entities and their business associates, a vast amount of health-related information does not fall within the HIPAA regulatory framework and are not subject to privacy standards. The increasing presence of third-party consumer-facing apps has led to significant amounts of personal health information collected outside the HIPAA structure. This information should be afforded privacy and security protections that align with HIPAA. Creating new protections for this information, aligned with HIPAA, will build public trust in data collection while also supporting responsible use of information to improve health outcomes.

The Confidentiality Coalition appreciates the Federal Trade Commission's (FTC) emphasis on developing robust consumer privacy protections[1] and we encourage the FTC to explicitly examine steps to provide privacy standards for information that is used to support innovation,

[1] David Uberti, *FTC Vote Could Pave Way for New Privacy Rules*, The Wall Street Journal (July 1, 2021), https://www.wsj.com/articles/ftc-vote-could-pave-way-for-new-privacy-rules-11625171274.

improve health and health care delivery. A September 2020 survey[2] found that 90% of Americans are concerned about the privacy of their health data when not protected by HIPAA or other federal regulations. By implementing steps to protect this information, the FTC can help build back trust in information sharing.

Additionally, we encourage Congress to pass bipartisan national privacy legislation. Such legislation could grant FTC necessary authority to develop privacy regulations and provide stakeholders better clarity about how to sufficiently protect consumers' health information. Any privacy legislation should recognize the need to protect information not covered by HIPAA. The Confidentiality Coalition has developed "Beyond HIPAA" principles to govern the sharing of this information. These principles emphasize harmonization with HIPAA's privacy and security rules. They also advocate for prohibitions on the use of data beyond the expressed purpose for which consent was given, following a similar framework to HIPAA's privacy standards that permit use of PHI for healthcare treatment, payment, and operations. Developing legislative and regulatory solutions to protect consumers' health information not covered by the HIPAA rules will build trust in data collection, give stakeholders better certainty about how to protect such information, and ultimately help improve health outcomes.

The Confidentiality Coalition looks forward to working with you on steps to improve privacy protections for non-HIPAA health data. Please contact me at tgrande@hlc.org or 202-306-3538 with any questions.

Sincerely,

Tina O. Grande
Chair, Confidentiality Coalition and
Executive VP, Policy, Healthcare Leadership Council

[2] Ben Moscovitch, *Americans Want Federal Government to Make Sharing Electronic Health Data Easier*, The Pew Charitable Trusts (September 16, 2020), https://www.pewtrusts.org/en/research-and-analysis/articles/2020/09/16/americans-want-federal-government-to-make-sharing-electronic-health-data-easier.

Beyond HIPAA Privacy Principles

1. For the last 20 years, the HIPAA Privacy and Security Rules have engendered public trust that individually identifiable health information collected by providers and insurers (HIPAA covered entities) would be disclosed only for health functions like treatment, payment processing, and safety, and not used or disclosed for other purposes without an individual's authorization. Any future legislation or rulemaking that addresses individually identifiable health information should not conflict with HIPAA's Privacy and Security Rules.

    a. HIPAA's required "Notice of Privacy Practices" provides an overview of individuals' rights as well as permitted and required uses and disclosures of identifiable health information.

    b. HIPAA's approach requires use of risk-based administrative, technical, and physical safeguards allowing organizations the flexibility to implement policies and controls commensurate with the level of risks they have identified.

2. Congress should establish a single national privacy and security standard for *all* health information *not* subject to HIPAA. This single standard:

    a. Should not conflict with HIPAA,
    b. Should not disrupt day to day practices for HIPAA Covered Entities and Business Associates,
    c. Should align with HIPAA's definitions of health information, and
    d. Should adopt a risk-based approach for the development and implementation of security and privacy controls like HIPAA.

3. Individuals may not fully appreciate that individually identifiable health information collected outside of a HIPAA Covered Entity or Business Associate Agreement are not afforded HIPAA privacy and security protections. Individuals should be given clear, succinct notice concerning collection, use, disclosure, and protection of individually identifiable health information that is not subject to HIPAA.

4. Individual authorization processes (including revocation of authorization) for use and disclosure of identifiable health information not covered by HIPAA should be written in a meaningful and understandable manner and should be easily accessible to individuals prior to and after information is used or shared.

Effective date: May 2020

5. Entities that hold or collect identifiable health information have a responsibility to take necessary steps to maintain the trust of individuals. Entities that are not HIPAA Covered Entities or Business Associates that hold identifiable health information should clearly stipulate the purposes for which they collect, use, and disclose identifiable health information.

6. For data use and activities other than the purpose for which the data was provided, individuals must provide authorization for collection and use of individually identifiable health information. Such information collected, used or disclosed by entities outside of HIPAA should be limited to only that information needed to accomplish the purposes for data collection. This practice provides privacy protection while allowing for continued innovation.

7. Individuals should be informed of their right to seek redress – from the entity and from regulators – in the case of unauthorized access, misuse, or harm attributable to how their identifiable health information was collected, used or disclosed.

8. Penalties and enforcement must be meaningful in order to discourage misuse and unpermitted collection, use or disclosure of identifiable health information.