



January 24, 2020

The Honorable Frank Pallone Jr.  
Chairman  
U.S. House of Representatives  
Committee on Energy and Commerce  
2125 Rayburn House Office Building  
Washington, D.C. 20515

The Honorable Greg Walden  
Ranking Member  
U.S. House of Representatives  
Committee on Energy and Commerce  
2125 Rayburn House Office Building  
Washington, D.C. 20515

Dear Chairman Pallone and Ranking Member Walden:

The Confidentiality Coalition (Coalition) appreciates the opportunity to comment on the House Energy and Commerce Committee's recently released draft privacy legislation (Draft). We commend the Committee and its staff for working in a bipartisan manner to develop robust federal consumer privacy rights and protections.

The 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.

We understand that the Draft is a work-in-progress and that Committee staff are seeking to reach agreement on key components so that a final bill with bipartisan support can be introduced. We offer the below high-level comments and suggestions as the Committee continues to work towards this laudable goal.

**Preservation of HIPAA Framework**

The Health Insurance Portability and Accountability Act (HIPAA) has for over 20 years provided individuals with strong privacy rights and protections for their protected health

information.<sup>1</sup> Its well-established rules and guidance, together with robust and consistent enforcement by the Department of Health and Human Services, has made it a trusted and accepted national standard for the protection of personal health information. It has also provided HIPAA covered entities and their business associates with a clearly delineated framework and parameters within which to operate.

The Coalition has long supported federal legislation that would provide similar and harmonized strong national privacy and security protections for personal health information that is not protected by HIPAA. We have enclosed a copy of the Coalition's "Beyond HIPAA Privacy Principles" (Principles) which set forth our position on this for your consideration. The Coalition believes that any federal privacy bill should preserve the existing HIPAA framework, including implied consent for the use and disclosure of health information for treatment purposes, and minimum necessary information for payment and health care operation purposes. The HIPAA framework was carefully calibrated to recognize the unique nature of health information, and to ensure that its appropriate exchange for healthcare purposes continues without disruption while respecting patient privacy.

Therefore, while we support the Draft provisions that give individuals the opportunity to understand and make informed choices about how, with whom and for what purposes their personal information may be shared generally, which aligns with HIPAA privacy rules, we ask that any final privacy bill not apply to personal information already governed by HIPAA, as well as information intermingled with or indistinguishable from such information that is held by a HIPAA covered entity or business associate.

### **Harmonization with HIPAA**

It is also important that any federal privacy bill align with HIPAA concepts, definitions and standards. This will not only benefit consumers by providing them with the assurance of consistent treatment of all their health information, but is essential to ensure that health organizations covered by HIPAA, including business associates, are able to continue their day-to-day operations without disruption. For example, even if new federal privacy legislation appropriately excludes protected health information from its ambit, unless it defines de-identified data in a manner consistent with HIPAA, it could apply to data that meets the HIPAA standard of de-identification, but that may or may not meet the new legislation's definition of de-identified data. This unintended consequence could seriously impact the ability of healthcare organizations to aggregate and share health data for important public policy purposes such as developing evidence-based standards, quality metrics and standards, medical research, and management of healthcare delivery, to name only a few.

The great promise of interoperability – using technology to engage patients, deliver meaningful insights to help in the identification and diagnosis of disease, and guide treatment decisions - depends on the ability to appropriately share health data among HIPAA covered entities and others for these purposes. This promise cannot come to

---

<sup>1</sup> Only certain personal health information is protected by HIPAA. See definition of "protected health information" at 45 CFR 160.103.

fruition if these organizations are subject to, and constrained by, different standards that do not align or, potentially even conflict, with one another. This has proven to be a challenge for the appropriate sharing of patient substance use disorder information.<sup>2</sup> The investment of effort at the outset when crafting legislation so as to avoid this type of misalignment will yield significant dividends in the form of improved healthcare outcomes and quality of care, not to mention a more seamless and workable privacy framework for consumers and businesses alike. This is particularly pertinent today as the Administration seeks to execute on the requirements of the 21<sup>st</sup> Century Cures Act to improve health information interoperability with the goal of promoting greater data sharing among patients, healthcare providers, payers, researchers, and other healthcare entities. As the Office of the National Coordinator of Health Information Technology stated in its recently released draft 2020-2025 Federal Health IT Strategic Plan:

*[N]ew technologies, along with existing claims and EHR data, mean that the volume of health and health-related data being generated and available for improving care quality has never been greater. Collecting, organizing, analyzing, interpreting, and applying this “big data” to clinical decision making is both a challenge and a significant opportunity.<sup>3</sup>*

Finally, HIPAA de-identified information that may identify an individual healthcare provider should be exempt from an omnibus federal privacy law. This data is used in the context of patient safety, quality reporting, healthcare operations, and healthcare management. This includes, for example, reporting to peer review committees, quality improvement activities, adverse event reporting, communicable disease reporting, reporting of abuse and neglect, implementing product recalls, conduct of post-market surveillance for FDA-regulated products, regulatory compliance, and other public health purposes. This information is essential for protecting patient and public safety, improving healthcare quality and standards of care, and developing new approaches to identifying, diagnosing and combatting diseases. Congress and states have repeatedly recognized the importance of removing barriers to the reporting of this type of information, and any federal privacy legislation should similarly promote the sharing and analysis of such information for the purposes of enhancing patient safety, quality and public health, as well as to enable efficient and effective health delivery. Related to this, federal privacy legislation should similarly exclude personal information where the individual is acting in a business or professional context, such as identifiable information of healthcare providers included in patient records or submitted as part of patient safety and quality reporting.

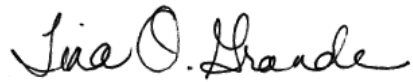
---

<sup>2</sup>The rules governing patient records subject to the Confidentiality of Substance Use Disorder Patient Records Regulations at 42 CFR Part 2 have significantly stricter express consent standards than HIPAA, causing some health care providers to refrain from sharing this information with others, even for treatment and care coordination purposes. The unintended consequence is that patients suffering from substance abuse disorders may receive more fragmented or delayed care.

<sup>3</sup> See the Office of the National Coordinator of Health Information Technology's [Draft 2020-2025 Federal Health IT Strategic Plan](#), p.12.

Thank you for the opportunity to provide comments on the Draft. We recognize the challenges in developing legislation on this important topic and stand ready to assist in any way we can. Please contact me at [tgrande@hlc.org](mailto:tgrande@hlc.org) or (202) 449-3433 if you have any questions or would like additional information.

Sincerely,

A handwritten signature in black ink that reads "Tina O. Grande". The signature is written in a cursive style with a large initial 'T' and 'G'.

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

Enclosure: Beyond HIPAA Privacy Principles



## 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 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.

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. Individuals must provide authorization for entities outside of HIPAA to collect 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.