Submitted electronically via **https://www.ehidc.org/resources/draft-consumer-privacy-framework-health-data**

September 30, 2020

Ms. Alice Leiter
Vice President and Senior Counsel
eHealth Initiative and Foundation
Alice@ehidc.org

Mr. Andrew Crawford
Policy Counsel
Center for Democracy &Technology Data and Privacy Project
acrawford@cdt.org

Re: Draft Consumer Privacy Framework for Health Data Comments

Dear Ms. Leiter and Mr. Crawford:

The Confidentiality Coalition appreciates the opportunity to submit comments on the "Proposed Consumer Privacy Framework for Health Data" by the eHealth Initiative (eHI) and Center for Democracy & Technology (CDT) that was released for public comment on August 27, 2020 (Draft Framework).

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 confidentiality protections for healthcare consumers. 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 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.

General Comments

Before commenting on specific sections of the Draft Framework, the Confidentiality Coalition would like to commend eHI and CDT for creating this proposal to address the gaps in the legal protections for health data outside the Health Insurance Portability and Accountability Act's (HIPAA) protections. We share the same concerns as eHI and CDT regarding the unregulated nature of this data and would like to underscore the need for a framework, ultimately regulatory in nature, to protect health records in the hands of non-HIPAA entities. As indicated in the Background section, this need has become more urgent since the issuance in May 2020 of the

Information Blocking final rule by the Department of Health and Human Services' (HHS) Office of the National Coordinator for Health Information Technology (ONC) and the Interoperability and Patient Access final rule by the Centers for Medicare and Medicaid Services (CMS). These rules will facilitate and accelerate the transfer of protected health information from HIPAA entities to non-HIPAA entities, such as third-party apps. While the intent is to give consumers greater control over their own health data, it will also result in many more health records falling outside of the strong protections of HIPAA, oftentimes without consumers understanding this or appreciating its implications.

The Confidentiality Coalition has long sought to advance a framework to protect personal health information that is not already covered by HIPAA. To this end, it has developed a set of privacy principles, "Beyond HIPAA Privacy Principles" (a copy of which is attached to these comments) that outline our views on the protection of this health data. As stated in these principles, the Confidentiality Coalition believes that health data falling outside HIPAA should be subject to uniform, national privacy and security rules comparable to HIPAA. To foster and retain consumer trust, the framework for these standards should ultimately be established through legislation enacted by Congress, with meaningful penalties and enforcement by a federal regulatory agency. However, until then, we support a voluntary framework that provides strong protections and harmonizes with HIPAA so as to facilitate compliance and the appropriate flow of health information.

Specific Comments
Below are our comments on some of the specific concepts and provisions in the Draft Framework.

1. Definitions
The Draft Framework defines and distinguishes between "consumer health information" (CHI), "aggregated data" and "de-identified data", noting that the latter two types of data pose fewer privacy risks. We support this distinction, and believe that it is important for participating entities to be encouraged to use aggregated or de-identified data wherever possible instead of CHI.

To ensure that this occurs, the definition of CHI should make clear that it is limited to information that can reasonably be linked to a unique individual or household. Device data should be included only to the extent that the device can in turn be linked to a unique individual or household. As currently written, paragraph a. of the definition of CHI requires that the information "relate" to an individual, but not necessarily an identified or reasonably identifiable individual. Similarly, the data sets listed in paragraph b. of the definition are not necessarily limited to data about an identified or reasonably identifiable individual. The definition of CHI should also clearly exclude aggregated data, de-identified data and publicly available information. To avoid confusion on this point, the Draft Framework should not refer to "aggregated consumer health information," "de-identified consumer health information" or "publicly available consumer health information." Similarly, the definitions of "aggregated data, "de-identified data" and "publicly available information" should each make clear that they are a not subsets of CHI and, in the case of de-identified data, that it cannot reasonably be linked to an "identified or identifiable" individual.

We also strongly encourage eHI and CDT to look to the HIPAA definition of de-identified data as the basis for the definition in the Draft Framework. The HIPAA definition provides two distinct methods or pathways for de-identifying protected health information, namely, the safe harbor method and the statistical expert method. Both methods are well established and well understood and provide specific standards that can be used by HIPAA entities to render

information de-identified. As currently written, the Draft Framework appears to require a method of de-identification similar to the HIPAA expert method, at least with respect to uses for research purposes, but does not provide for a simpler method, similar to the safe harbor method, that would not require the use of a statistical expert. Providing similar de-identifications standards to those in HIPAA, and regardless of the purpose for which the de-identified data is used, would allow participating entities to draw on the experience gained in HIPAA. It would also provide consumers with the assurance that consistent and robust standards for de-identification are applied before broader use of the data is permitted. While there is no definition of "aggregated data" in HIPAA, it would be similarly helpful to provide clear standards or criteria for data to qualify as aggregated, and through a simpler methodology than statistical analysis. It would also be helpful if the definition made clear whether aggregated data is intended to be distinguishable from aggregated de-identified data and, if so, how.

Finally, consistent with the Background and Project Goals and Status sections, which make clear that the intent of the Draft Framework is to address health data "outside HIPAA's coverage," the definition of CHI should explicitly exclude protected health information governed by HIPAA.

2. Use of Aggregated and De-identified Data

The Confidentiality Coalition is mindful that aggregating or de-identifying data is not a "silver bullet" in that there still remains a risk of re-identification, however small. However, consistent with the goal of encouraging the use of aggregated and de-identified data instead of identifiable data wherever possible, we recommend that the Draft Framework allow aggregated data to fall outside the framework in the same way as de-identified data falls outside of HIPAA. As written, it appears that aggregated data may be used only for research purposes, and that participating entities could not even request consumers to consent to the use of such data more broadly. This would exclude the use of such data for many beneficial purposes such as training, quality assurance, population health, safety evaluations, products or service improvement, to name only a few.

While the definition of de-identified data does not limit its use for research purposes, and the comment in the section on "Permissible Collection and Use Practices" suggests that de-identified data could be used for "current behavioral advertising and commercial product development activities," there is no exception in Section V for this purpose. There is also no general exception for use of de-identified data. Such an exception and the exclusion of de-identified data from CHI would make clear to participating entities that they may use such data for any lawful purpose.

3. Use of Publicly Available Information

The Confidentiality Coalition agrees that there is individual and societal value to the free flow of information that has legitimately been made public. Therefore, while we agree that publicly available information should not be permitted to be used for discriminatory purposes as appears to be the intent of the exception in Section V.1.d, we are concerned that this may be read to limit publicly available information to only the purposes specified in the exception. For example, publicly available information on physicians and other healthcare professionals is currently used for valuable public policy purposes, including quality improvement and evaluation, and these types of uses should continue to be permitted. While we do not believe the definition of CHI is intended to encompass this type of data or that the Draft Framework is intended to limit the use of such data for lawful purposes, we recommend that the Draft Framework make clear that publicly available information falls outside its ambit to avoid confusion or have a chilling effect on the many beneficial uses of publicly available information.

4. Transparency and Notice
We agree that transparency and notice to consumers are essential in order for consumers to be able to make informed decisions regarding the disclosure of their health information. A clear and simple description of an entity's data collection and use practices and a consumer's data rights is also critical in order to be able to move away from reliance on a consent-based model. We particularly support the concept of a layered or two-tier notice for consumers. This would allow a consumer to learn, through a succinct and consumer-friendly cover or first notice, of their data rights and the key privacy practices of a participating entity, with a second more detailed notice being available to provide additional information on the entity's privacy practices, and information on how consumers may exercise their data rights.

However, we are concerned that requiring a listing by name of every entity with which the participating entity has or will share CHI is not practicable or even helpful to consumers. In addition, there are many different reasons – some in the public interest, but others potentially not – that other entities, including competitors, may be interested in this type of information, and it is not clear that these entities, other than regulators, should have an automatic right to know this level of detail. The Draft Framework could potentially include a consumer right to request certain information about non-routine disclosures that the participating entity makes of CHI generally. This would strike a reasonable balance between the consumer's interest and the administrative burden on the participating entity.

5. Consent
The Confidentiality Coalition strongly supports the goal of moving "beyond outdated notice and consent models" so as to "shift the burden of privacy risk off consumers." Such an approach is consistent with the approach in HIPAA, which allows use of protected health information for treatment, payment and healthcare operations after the provision of the covered entity's notice of privacy practices but without requiring an individual's affirmative consent or authorization. Similarly, in the Draft Framework, participating entities should be required to provide a clear and concise notice of their data collection and use practices to consumers and then be permitted to use a consumer's CHI for the purposes for which it was provided by the consumer (i.e., consistent with the consumer's reasonable expectations in the circumstances) without having to obtain the consumer's affirmative express consent. Any other use outside of the original purpose and expectations should require the consumer's affirmative express consent, subject to limited exceptions for public policy purposes similar to those allowed in HIPAA. In addition, when CHI is shared for a public policy purpose, the recipient of the CHI should be limited to using and disclosing the data only for the public policy purpose for which it was provided to the entity. We share the concern about blanket consents that would allow use of CHI "for a host of possible uses," and therefore, agree that any affirmative express consent should be specific and narrowly construed.

However, we do not believe that obtaining written consent for uses that are consistent with a consumer's request or reasonable expectations is beneficial or meaningful. This would simply perpetuate the outdated consent model where consumers are required in a rote fashion to check boxes or sign forms before being able to proceed. This approach imposes administrative burdens and operational hurdles without any commensurate consumer benefit and, indeed, would only create the illusion of consumer control. As in the HIPAA framework, consumers that choose to request or use certain products or services that require use of their health data should reasonably expect that their health data will be used to support the provision of those products or services.

6. Service Providers
The Draft Framework states that participating entities must make "reasonable efforts to ensure" that third parties with whom they share CHI meet the obligations of this framework. The Confidentiality Coalition supports requiring service providers to be subject to the same obligations as the participating entity. Given the relationship, and similar to the HIPAA approach to business associates, we believe that the Draft Framework should affirmatively require that service providers be bound to the same obligations through a written agreement. In addition, participating entities should have responsibility for ensuring compliance with the Draft Framework by their service providers. This could include requiring an initial evaluation of the service provider's privacy and security capabilities, as well as ongoing monitoring of service providers through periodic audits or third-party assessments.

With respect to third parties that are not service providers, a "reasonable efforts" standard to obtain a similar contractual commitment to comply with the framework may be appropriate for some third parties, but not others. For example, in the case of disclosures to government agencies or in legal proceedings, it may not be feasible or appropriate to require the third party to agree to comply with the framework. In addition, while participating entities may ensure that third parties commit to complying with the framework, they will generally not be in a position to "ensure" such compliance with third parties that are not service providers.

7. Security
The Confidentiality Coalition supports the inclusion of security requirements in the Draft Framework. Even though the primary focus of the framework is on privacy protections, without reasonable security standards a privacy framework will have little value. We also strongly support the flexible, outcome-based scaled approach described in the Draft Framework, which appropriately takes into account the sensitivity of the data, the nature of its uses and the state of technology.

8. Proposed Structure of the Framework
The Confidentiality Coalition supports the program's emphasis on robust initial vetting and ongoing accountability. We agree that this is critical to ensure that the program does not become a shield for bad actors or viewed as no more than a rubber stamp for dues-paying members. In light of this, we recommend that the Draft Framework provide at least a high-level description of the process and standards that will be involved in the initial onboarding and ongoing audits and assessments.

Finally, we believe a rigorous and independent onboarding and ongoing monitoring process is essential to engender the necessary consumer buy-in and trust. This trust, and the program's viability as an interim substitute for legislation, will depend on the program's certifying entity, as well as that of any program staff and auditing entities, being transparently independent. Therefore, greater clarity on the criteria and process to determine and maintain this independence would be helpful to build confidence in the Draft Framework.

The Coalition appreciates the opportunity to provide comments on the Draft Framework and stands ready to work with eHI and CDT as they seek to finalize it. Once implemented, we believe such a framework can begin to provide meaningful protections for health data until such time as comprehensive national privacy legislation can be enacted. Please contact me at tgrande@hlc.org or at (202) 449-3433 if there are any comments or questions about the comments in this letter.

Sincerely,

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

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.