



**GENERAL COMMITTEE MEETING**

**Thursday, January 17, 2019**

3:00 PM to 4:00 PM

Healthcare Leadership Council

750 9th Street, NW, Suite 500 Washington, D.C. 20001

**Conference Line:** 857-232-0157, **Code:** 30-40-73

1. **Welcome and Introductions**
2. **HIPAA RFI** **Attachment 1**
3. **Principles on Privacy** **Attachment 2**
4. **NIST RFI Comments:**  
*Developing A Privacy Framework* **Attachment 3**

**Proposals Discussed in the HIPAA RFI**

- 1) Creating a requirement for Covered Entity health care providers to respond to requests for patient records from other Covered Entity health care providers for purposes of treatment, care coordination or case management;
- 2) Excepting disclosures of PHI to Covered Entities for care coordination and case management from the minimum necessary requirement;
- 3) Establishing an express regulatory permission for Covered Entities to disclose PHI to social service agencies or community-based support programs;
- 4) Revisiting whether health care clearinghouses should be considered Business Associates of Covered Entity health care providers when processing claims, and whether health care clearinghouses should be directly subject to requirements to provide individuals with access to PHI;
- 5) Establishing new disclosure pathways for Covered Entities to share PHI with family members, caregivers, and others in a position to avert threats of harm to health and safety, or when necessary to promote the health and recovery of individuals with substance use disorders or serious mental illness, including potential changes to the personal representative pathway.
- 6) Withdrawing the previous May 2011 Notice of Proposed Rulemaking that proposed to establish a new patient right to an “access report” listing each time the individual’s information in an electronic designated record set was accessed – whether the access constituted a “use” or a “disclosure”, and requesting information to be used in replacing the access report proposal with a revised proposal to implement the HITECH requirement to expand the HIPAA Privacy Rule’s accounting of disclosures requirement to include disclosures through an Electronic Health Record (EHR) over the previous three years for treatment, payment and health care operations; and
- 7) Establishing a safe harbor for using OCR’s Model Notice of Privacy Practices, and eliminating or modifying the obligation for health care providers to make a good faith effort to obtain an acknowledgment of the receipt of the provider’s Notice of Privacy Practices upon the individual’s first visit.
- 8) A request for public input on ways to modify HIPAA to remove regulatory obstacles and decrease regulatory burdens in order to facilitate efficient care coordination and/or case management and promote the transformation to value-based health care while preserving the privacy and security of PHI. The Coalition could, for example, consider commenting on the following:
  - a. Modernizing the pathway that allows Covered Entities to disclose PHI to researchers for activities that are preparatory to research studies.

Expanding the definition of “Organized Health Care Arrangement” or broadening the permitted health care operations under 45 C.F.R. § 164.506(c)(4) to account for value-based pricing arrangements between.



## PRINCIPLES ON PRIVACY

1. All care providers have a responsibility to take necessary steps to maintain the confidentiality and trust of patients as we strive to improve healthcare quality.
2. The framework established by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule should be maintained. HIPAA established a uniform framework for acceptable uses and disclosures of individually-identifiable health information within healthcare delivery and payment systems for the privacy and security of health information.
3. HIPAA, through “implied consent,” permits the sharing of medical information for specified identified healthcare priorities which include treatment, payment and healthcare operations. This model has served patients well by ensuring quick and appropriate access to medical care, especially in emergency situations where the patient may be unable to give written consent.
4. The Privacy Rule requires that healthcare providers and health plans limit disclosure of protected health information to the minimum necessary to pay for healthcare claims and other essential healthcare operations. *[What kind of statement do we want to make about min. necessary?]*
5. Personal health information must be secured and protected from misuses and inappropriate disclosures under applicable laws and regulations.
6. Providers should have as complete a patient’s record as necessary to provide care. Having access to a complete and timely medical record allows providers to remain confident that they are well-informed in the clinical decision-making process.
7. A privacy framework should be consistent nationally so that providers, health plans, and researchers working across state lines may exchange information efficiently and effectively in order to provide treatment, extend coverage, and advance medical knowledge, whether through a national health information network or another means of health information exchange.
8. The timely and accurate flow of de-identified data is crucial to achieving the quality-improving benefits of national health information exchange while protecting individuals’ privacy. Federal privacy policy should be consistent with the HIPAA regulations for the de-identification and/or aggregation of data to allow access to properly de-identified information. This allows researchers, public health officials, and others to assess quality of care, investigate threats to the public’s health, respond quickly in emergency situations, and collect information vital to improving healthcare safety and quality.
9. For the last 20 years, HIPAA has engendered consumer trust. Any future rulemaking that addresses identifiable health information should conform with consumers’ expectations.



## **SUBMITTED ELECTRONICALLY**

January 14, 2019

Katie MacFarland  
National Institute of Standards and Technology  
100 Bureau Drive  
Stop 2000  
Gaithersburg, MD 20899

**RE: Docket No. 181101997-8997-01: Developing a Privacy Framework**

Dear Sir or Madam:

The Confidentiality Coalition respectfully submits these comments in response to the National Institute of Standards and Technology's ("NIST's") request for information to help identify, understand, refine and guide the development of NIST's Privacy Framework (the "Proposed 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 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 have attached additional information about the Coalition and its membership as [Appendix A](#) to this letter.

The Confidentiality Coalition welcomes NIST's efforts to develop a voluntary, non-prescriptive tool to assist organizations in assessing their privacy risks and achieving desired privacy outcomes. As the Coalition noted in its comments to the Department of Commerce's Request for Comment on the Administration's Approach to Consumer Privacy, the Coalition believes a risk-based approach could provide flexibility to organizations to implement privacy policies and controls commensurate with the level of

privacy risk they have identified through the framework. In practice, however, the success of such an approach will depend on the certainty organizations can have that what they are doing to comply with the approach is sufficient. Without such certainty, organizations may find a risk-based approach too uncertain – as the process for determining the appropriate privacy controls and policy will be difficult to predict and verify.

To reduce the potential burdens of a risk-based approach, the Proposed Framework should, in addition to helping organizations identify privacy risks, provide guidance on different ways that organizations could achieve the desired privacy “outcomes” using the tool. For example, if based on the tool an organization were to determine that consumers should be provided choice prior to certain disclosures of their information, the organization should also be able to identify through the tool different acceptable methods for providing this choice to the consumers.

### ***Harmonization With HIPAA and Other Existing Privacy Frameworks***

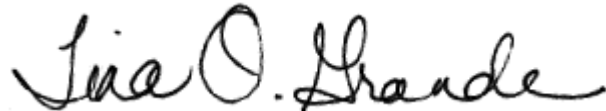
Many of the Coalition’s members are already regulated as Covered Entities or Business Associates under the HIPAA Privacy Rule, and therefore are required to follow a set of *prescriptive* privacy requirements that are based on the Fair Information Practice Principles. We encourage NIST to ensure that the Proposed Framework harmonizes with the prescriptive obligations of HIPAA and other existing privacy frameworks, as we believe consumers expect their information to be protected in a similar manner whether handled by entities currently regulated by existing privacy frameworks like HIPAA or otherwise.

For example, Covered Entities are required to put in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information, and to limit incidental uses or disclosures made pursuant to otherwise permitted or required uses or disclosures of protected health information (PHI). This provision requires Covered Entities to analyze the potential privacy risks to PHI (in paper or electronic form), and implement policies and procedures to mitigate against such risks. Our members who are Covered Entities or Business Associates would be more likely to use the Proposed Framework if they have assurances from NIST and the Office for Civil Rights for the U.S. Department of Health and Human Services that they could use it to meet these assessment obligations under HIPAA.

Covered Entities and Business Associates further rely on HIPAA’s de-identification standard to remove identifying information and protect the privacy of patients and health plan beneficiaries. Under HIPAA’s de-identification standard, the Covered Entity (or Business Associate with proper permission) may either remove 18 specific identifiers listed in the HIPAA Privacy Rule (the “Safe-Harbor Method”), or hire a statistical expert to review the data set or the proposed methodology of de-identification (the “Expert Determination Method”). As the HIPAA de-identification methodologies are widely used both within and outside of the healthcare industry, we recommend that NIST recognize these methodologies as acceptable for protecting consumer privacy under the Proposed Framework.

Overall, we are supportive of NIST's efforts to develop a voluntary, non-prescriptive Privacy Framework that would assist organizations in their efforts to identify and manage privacy risks. We hope the Proposed Framework will complement existing prescriptive frameworks like HIPAA, and not create a conflicting set of standards. Our members look forward to the opportunity to work with NIST in the development of the Proposed Framework through the collaborative process that NIST has established to solicit stakeholder feedback.

Sincerely,

A handwritten signature in black ink that reads "Tina O. Grande". The signature is written in a cursive style with a large, looped initial "T".

Tina Grande

Enclosure



### **ABOUT THE CONFIDENTIALITY COALITION**

The Confidentiality Coalition is a broad group of organizations working to ensure that we as a nation find the right balance between the protection of confidential health information and the efficient and interoperable systems needed to provide the very best quality of care.

The Confidentiality Coalition brings together 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, clinical laboratories, home care providers, patient groups, and others. Through this diversity, we are able to develop a nuanced perspective on the impact of any legislation or regulation affecting the privacy and security of health consumers.

We advocate for policies and practices that safeguard the privacy of patients and healthcare consumers while, at the same time, supporting policies that enable the essential flow of information that is critical to the timely and effective delivery of healthcare. Timely and accurate patient information leads to both improvements in quality and safety and the development of new lifesaving and life-enhancing medical interventions.

Membership in the Confidentiality Coalition gives individual organizations a broader voice on privacy and security-related issues. The coalition website, [www.confidentialitycoalition.org](http://www.confidentialitycoalition.org), features legislative and regulatory developments in health privacy policy and security and highlights the Coalition's ongoing activities.

For more information about the Confidentiality Coalition, please contact Tina Grande at [tgrande@hlc.org](mailto:tgrande@hlc.org) or 202.449.3433.



### MEMBERSHIP

AdventHealth	Healthcare Leadership Council
Aetna, a CVS Health business	Hearst Health
America's Health Insurance Plans	HITRUST
American Hospital Association	Intermountain Healthcare
American Society for Radiation Oncology	IQVIA
AmerisourceBergen	Johnson & Johnson
Amgen	Kaiser Permanente
AMN Healthcare	Leidos
Anthem	LEO Pharma
Ascension	Mallinckrodt Pharmaceuticals
Association of American Medical Colleges	Marshfield Clinic Health System
Association of Clinical Research Organizations	Maxim Healthcare Services
athenahealth	Mayo Clinic
Augmedix	McKesson Corporation
Bio-Reference Laboratories	Medical Group Management Association
Blue Cross Blue Shield Association	Medidata Solutions
BlueCross BlueShield of Tennessee	Medtronic
Cardinal Health	MemorialCare Health System
Cerner	Merck
Change Healthcare	MetLife
Children's Hospital of Philadelphia (CHOP)	National Association for Behavioral Healthcare
CHIME	National Association of Chain Drug Stores
Cigna	NewYork-Presbyterian Hospital
City of Hope	NorthShore University Health System
Cleveland Clinic	Pfizer
College of American Pathologists	Pharmaceutical Care Management Association
Comfort Keepers	Premier healthcare alliance
ConnectiveRx	SCAN Health Plan
Cotiviti	Senior Helpers
CVS Health	State Farm
Datavant	Stryker
dEpid/dt Consulting Inc.	Surescripts
Electronic Healthcare Network Accreditation Commission	Teladoc
EMD Serono	Texas Health Resources
Express Scripts	UCB
Fairview Health Services	UnitedHealth Group
Federation of American Hospitals	Vizient
Genetic Alliance	Workgroup for Electronic Data Interchange
Genosity	ZS Associates