



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,

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, features legislative and regulatory developments in health privacy policy and security and highlights the Coalition's ongoing activities.



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