April 28, 2020

The Honorable Stephen M. Hahn, M.D.
Commissioner
U.S. Food and Drug Administration
10903 New Hampshire Avenue
Silver Spring, MD 20857

Dear Commissioner Hahn:

On behalf of the Confidentiality Coalition, thank you for addressing the important issue of modernizing the U.S. Food and Drug Administration's (FDA's) data strategy. Issues such as data stewardship, data exchange, data analytics and data quality are paramount to ensuring that the information gathered through various means both inside and outside of the healthcare system can be utilized in an appropriate, efficient manner to improve the well-being and health outcomes of individuals and populations.

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.

The Confidentiality Coalition strongly supports an innovative healthcare system that harnesses data to elevate the quality of care delivery, turbocharges medical research, and enables greater efficiencies within the system. We are in a golden era of research and development, leading to treatments and technologies that are conquering disease and extending lives.

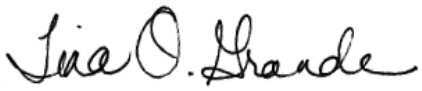
With this in mind, the Confidentiality Coalition's core approach to stewardship of healthcare data is that all care providers, health plans, and other entities that generate, hold, manage, exchange and share health data have a responsibility to take necessary steps to maintain the confidentiality and trust of patients and consumers. Our members believe that the framework established by the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules has proven an effective means of maintaining trust and accountability, and as such, it should be maintained.

As you know, not all health information is protected under the HIPAA privacy and security rules. To safeguard individuals' health information when it is not protected under HIPAA, our members advocate for a national framework, based upon and harmonized with HIPAA, to establish a uniform approach for acceptable uses and disclosures of individually-identifiable health information. Attached to this letter is the Confidentiality Coalition's "Beyond HIPAA Privacy

Principles." We encourage you to address data stewardship and modernizing the FDA's data strategy through the lens of these principles.

In closing, we appreciate the opportunity to share with you these important principles that reflect the position of the Confidentiality Coalition's membership, which spans all sectors of the healthcare system. We look forward to working with the FDA on issues related to data strategy and modernization. If you have any questions, please contact me at tgrande@hlc.org.

Sincerely,



Tina Olson Grande
Executive Vice President, Policy
Healthcare Leadership Council
On behalf of the Confidentiality Coalition

Enclosure(s)

CONFIDENTIALITY COALITION

MEMBERSHIP

AdvaMed
AdventHealth
America's Health Insurance Plans
American Hospital Association
American Society for Radiation Oncology
AmerisourceBergen
Amgen
AMN Healthcare
Anthem
Ascension
Association of American Medical Colleges
Association of Clinical Research Organizations
athenahealth
Augmedix
Blue Cross Blue Shield Association
BlueCross BlueShield of North Carolina
BlueCross BlueShield of Tennessee
Cerner
Change Healthcare
CHIME
Cigna
Ciox Health
City of Hope
CLEAR
Cleveland Clinic Foundation
College of American Pathologists
ConnectiveRx
Cotiviti
CVS Health
Datavant
dEpid/dt Consulting Inc.
EMD Serono
Express Scripts
Fairview Health Services
Federation of American Hospitals
Genentech
Genetic Alliance
Genosity
Guardant
Healthcare Leadership Council
Health Management Systems
HITRUST
Intermountain Healthcare
IQVIA
Johnson & Johnson
Kaiser Permanente
Leidos
Mallinckrodt
Marshfield Clinic Health System
Mayo Clinic
McKesson Corporation
Medical Group Management Association
Medidata Solutions
Medtronic
MemorialCare Health System
Millennium Health
Memorial Sloan Kettering Cancer Center
Merck
MetLife
National Association of Chain Drug Stores
National Community Pharmacists Association
NewYork-Presbyterian Hospital
NorthShore University HealthSystem
Pfizer
Pharmaceutical Care Management Association
Premier healthcare alliance
SCAN Health Plan
Senior Helpers
SSM Health
State Farm
Stryker
Surescripts
Teladoc Health
Texas Health Resources
Tivity Health
UCB
UnitedHealth Group
Vineti
Vizient
Workgroup for Electronic Data Interchange
ZS Associates

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.