December 4, 2019

The Honorable Roger Wicker
Chairman
U.S. Senate Committee on Commerce,
Science, and Transportation
512 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Maria Cantwell
Ranking Member
U.S. Senate Committee on Commerce,
Science, and Transportation
512 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Wicker and Ranking Member Cantwell:

Thank you for holding a hearing on "Examining Legislative Proposals to Protect Consumer Data Privacy." The Confidentiality Coalition appreciates the opportunity to share its thoughts with you on this important issue.

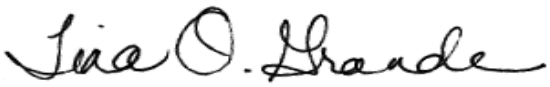
The Confidentiality Coalition is composed of a broad group of hospitals, medical teaching colleges, health plans, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health product distributors, pharmacies, pharmacy benefit managers, health information and research organizations, patient groups, and others founded to advance effective patient confidentiality protections. The Coalition's mission is to advocate for 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 Health Insurance Portability and Accountability Act (HIPAA) established acceptable uses and disclosures of individually identifiable health information within healthcare delivery and payment systems for the privacy and security of health information. The Confidentiality Coalition believes that to the extent not already provided under HIPAA, privacy rules should apply to all individuals and organizations that create, compile, store, transmit, or use personal health information. New innovations in health information technology (mobile health apps, wearable devices, etc.) have empowered consumers to be more engaged in managing their health outside of traditional healthcare settings. However, this technology is often not offered by or on behalf of covered entities; but rather are offered as direct to consumer services. Consumers 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.

As the committee continues to explore legislative proposals to protect consumer data privacy, we are pleased to share the Confidentiality Coalition's "Beyond HIPAA" Privacy Principles that convey our views on the protection of health information that is not subject to HIPAA.

Thank you for examining this important issue and please feel free to contact Tina Grande, at (202) 449-3433 or tgrande@hlc.org with any questions. Enclosed you will find information on the Confidentiality Coalition, the Confidentiality Coalition's "Beyond HIPAA" Privacy Principles, and a list of coalition members.

Sincerely,



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

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.

For more information about the Confidentiality Coalition, please contact Tina Grande at tgrande@hlc.org or 202.449.3433.

CONFIDENTIALITY COALITION

MEMBERSHIP

AdvaMed
AdventHealth
Aetna, a CVS Health business
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
Bio-Reference Laboratories
Blue Cross Blue Shield Association
BlueCross BlueShield of North Carolina
BlueCross BlueShield of Tennessee
Cerner
Change Healthcare
Children's Hospital of Philadelphia (CHOP)
CHIME
Cigna
Ciox Health
City of Hope
Cleveland Clinic
College of American Pathologists
Comfort Keepers
ConnectiveRx
Cotiviti
CVS Health
Datavant
dEpid/dt Consulting Inc.
Electronic Healthcare Network Accreditation Commission
EMD Serono
Express Scripts
Fairview Health Services
Federation of American Hospitals
Genentech
Genetic Alliance
Genosity
Healthcare Leadership Council
Health Management Systems
Hearst Health
HITRUST
Intermountain Healthcare
IQVIA
Johnson & Johnson
Kaiser Permanente
Leidos
Mallinckrodt Pharmaceuticals
Marshfield Clinic Health System
Mayo Clinic
McKesson Corporation
Medical Group Management Association
Medidata Solutions
Medtronic
MemorialCare Health System
Merck
MetLife
National Association for Behavioral Healthcare
National Association of Chain Drug Stores
National Community Pharmacists Association
NewYork-Presbyterian Hospital
NorthShore University Health System
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

Revised November 2019

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.