



May 8, 2019

The Honorable Janice D. Schakowsky
Chairman
U.S. House of Representatives
Committee on Energy and Commerce
Consumer Protection and Commerce Subcommittee
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Cathy McMorris Rodgers
Ranking Member
U.S. House of Representatives
Committee on Energy and Commerce
Consumer Protection and Commerce Subcommittee
2125 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Schakowsky and Ranking Member McMorris Rodgers:

The Confidentiality Coalition appreciates the opportunity to submit this letter to the U.S. House of Representatives Consumer Protection and Commerce Subcommittee hearing, "Oversight of the Federal Trade Commission: Strengthening Protections for Americans' Privacy and Data Security."

We are a broad group of organizations—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, patient groups, home care providers, and others—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 high quality care.

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 be consistent so that persons and organizations not covered by HIPAA that create, compile, store, transmit, or use health information operate under a similar expectation of acceptable uses and disclosures.

The Confidentiality Coalition has long supported the Federal Trade Commission's (FTC) oversight of personal health records (PHR) that reside in non-HIPAA covered entities, which was provided in the Health Information Technology for Economic and Clinical Health (HITECH) Act (Pub L. No. 111-5 §

13407). As required by HITECH, the FTC promulgated rules to carry out this authority. In 2010, the FTC finalized a Health Breach Notification Rule that requires vendors of PHRs, PHR-related entities, and third-party service providers for a vendor of PHRs to notify the FTC in the event of a breach. As the committee continues to explore the government's role in strengthening protections for Americans' privacy and data security, the coalition supports a federal data privacy framework that is consistent nationally and includes similar expectations to that of HIPAA for acceptable uses and disclosures for non-HIPAA covered health information. This is vital to maintain consumer trust in the healthcare system.

Thank you for examining this important issue and please feel free to reach out to Tina Olson Grande, Senior Vice President for Policy at the Healthcare Leadership Council on behalf of the Confidentiality Coalition, at (202) 449-3433 or tgrande@hlc.org with any questions. Enclosed you will find the Confidentiality Coalition's Principles on Privacy and a list of coalition members.

Sincerely,

A handwritten signature in black ink that reads "Tina O. Grande". The signature is written in a cursive, flowing style.

Tina Olson Grande
Healthcare Leadership Council on behalf of the Confidentiality Coalition

Enclosure



CONFIDENTIALITY COALITION

MEMBERSHIP

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
Cardinal Health
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
Genetic Alliance
Genosity
Healthcare Leadership Council
Hearst Health
HITRUST
Intermountain Healthcare
IQVIA
Johnson & Johnson
Kaiser Permanente
Leidos
Mallinckrodt Pharmaceuticals
Marshfield Clinic Health System
Maxim Healthcare Services
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
State Farm
Stryker
Surescripts
Teladoc
Texas Health Resources
Tivity Health
UCB
UnitedHealth Group
Vizient
Workgroup for Electronic Data Interchange
ZS Associates



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 to enable the provision of health care services to patients. HIPAA follows the widely accepted Fair Information Practices standards (FIPS.)
 - a. The HIPAA Privacy Rule, through “implied consent,” permits the sharing of medical information for specified identified healthcare priorities which include treatment, payment and healthcare operations (as expected by patients seeking medical care.) 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.
 - b. The HIPAA 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. This practice provides privacy protection while allowing for continued operations. Minimum necessary is relatively easy and simple to administer and practice.
3. Personal health information must be secured and protected from misuses and inappropriate disclosures under applicable laws and regulations.
4. 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.
5. Privacy frameworks should be consistent nationally and across sectors so that providers, health plans, and researchers working across state lines and with entities governed by other privacy frameworks 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.
6. 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.
7. For the last 20 years, the HIPAA privacy standards have engendered consumer trust. Any future legislation or rulemaking that addresses identifiable health information should conform with consumers’ expectations.