SUBMITTED ELECTRONICALLY

February 11, 2019

U.S. Department of Health and Human Services
Office for Civil Rights
Hubert H. Humphrey Building
Room 509F
200 Independence Avenue SW
Washington, DC 20201

RE: Request for Information, RIN 0945-AA00

Dear Sir or Madam:

The Confidentiality Coalition respectfully submits these comments in response to the Office for Civil Rights' ("OCR's") Request for Information to assist OCR in identifying provisions of the Privacy and Security Rules, promulgated pursuant to the Health Insurance Portability and Accountability Act ("HIPAA"), that impede the transformation to value-based healthcare or that limit or discourage coordinated care among individuals and Covered Entities without meaningfully contributing to the protection of the privacy or security of individuals' PHI (the "RFI").

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.

COMMENTS

The Confidentiality Coalition appreciates the opportunity to respond to OCR's Request for Information concerning HIPAA. The Coalition agrees with OCR that it is prudent to

review and assess the HIPAA Privacy and Security Rules at this time given the rapid evolution of the provision of healthcare and the rise of value-based payment models, although we believe that several of the barriers discussed in the RFI may be better addressed through guidance and education rather than through regulation.

We also believe alignment between HIPAA and non-preempted state and federal laws would help solve many of the perceived barriers discussed in the RFI. The vast array of state laws pertaining to the handling of health information makes it difficult for Covered Entities to catalogue and comply with all 50 states' laws. Some states require healthcare providers to obtain a consent before disclosing any health information, including for treatment, payment and healthcare operations purposes. Other states generally permit disclosures between healthcare providers and health plans without a consent, but require consent before any disclosure of sensitive categories of information, such as mental health, HIV testing results, genetic information, and information about sexually transmitted diseases. States define the information in these sensitive categories differently, making it difficult for healthcare providers and health plans to develop strategies for complying with the consent requirements – particularly when disclosing health information across state lines. As a result of these complex state and federal legal requirements that are not pre-empted by HIPAA, some healthcare providers and health plans default to requiring a consent or authorization prior to disclosing PHI – even for treatment, payment and healthcare operations purposes. Privacy laws that are not pre-empted by HIPAA create barriers to the seamless sharing of PHI for case management and care coordination, and the implementation of value-based payment models. While we understand a statutory change may be needed to change how HIPAA interacts with other state and federal laws, we believe patients, plan beneficiaries, and their families would benefit if HIPAA's framework globally applied to all PHI.

I. Promoting Information Sharing for Treatment and Care Coordination

The Coalition believes that OCR should retain the current timing requirements for providing individuals with access to their Designated Record Sets, as Covered Entities need time to accommodate situations where it is difficult and more time consuming to retrieve information requested by the individual.

While the Coalition believes Covered Entities typically are able to provide PHI to individuals more quickly than thirty (30) days, and indeed do so, the Coalition would have significant concerns with any proposal that shortens the upper time limit for providing individuals with access to their PHI. For example, there are situations where an individual requests medical records from legacy electronic systems that are only accessible through remotely stored physical back-up tapes. In other situations, an individual may not only ask for copies of information within his or her medical record, but also any e-mail correspondence among healthcare providers about the patient's case. Covered Entities need additional time in order to process these access requests fully and accurately.

The Coalition believes that Covered Entities respond to requests quicker than thirty (30) days when they are able to do so. Therefore, the Coalition does not feel that it is necessary to shorten the timeliness requirement.

If OCR were to propose shortening the 30-day time limit, this would require additional staffing and retraining for employees of Covered Entities and Business Associates. Should OCR take this approach, the Coalition asks that OCR permit Covered Entities to extend the shorter time limit to account for challenges like the examples we have provided above.

The Coalition supports policies that allow individuals to receive access to their PHI directly from Business Associates, such as healthcare clearinghouses. The Coalition does not believe, however, that it is prudent or in the interest of the public that healthcare clearinghouses receive special rights to PHI beyond those typically given to other Covered Entities or their Business Associates.

The Coalition supports efforts to improve patient access to health information in a manner that makes it easier for providers and patients to aggregate PHI from multiple providers. Section 4006 of the 21st Century Cures Act modified the HITECH Act to permit Business Associates to provide electronic access to PHI directly to individuals when the individual requests access to such information directly from the Business Associate. In our view, Congress's goal in including this provision in the 21st Century Cures Act was to allow Business Associates who maintain PHI electronically on behalf of a Covered Entity – such as an electronic health record vendor, healthcare clearinghouse or health information exchange – to respond directly to individuals' requests for access to their PHI if they so choose. The Coalition believes that modifications to the HIPAA Privacy Rule consistent with this statutory change would adequately address the concerns raised by healthcare clearinghouses and other Business Associates about providing PHI to individuals directly and avoid the downsides to the proposal in the RFI.

The PHI provided to a healthcare clearinghouse or most other Business Associates originates with a healthcare provider or a payor. Individuals are unable to select their healthcare clearinghouses and rely on their healthcare providers and health plans to select service providers that will protect their PHI. The Business Associate Agreement requirement allows healthcare providers and health plans to make healthcare clearinghouses accountable for how they use, disclose, and secure their patients' and beneficiaries' PHI. As a result, the Coalition does not believe it would improve patient access or patient privacy to eliminate the requirement for healthcare clearinghouses to enter into Business Associate Agreements with the healthcare providers and health plans they assist with claims submission.

The Coalition expressed opposition to recent legislative proposals concerning healthcare clearinghouses that would not only have eliminated the requirement for healthcare providers and payors to enter into Business Associate Agreements with clearinghouses, but also would have invalidated *existing* Business Associate Agreements between healthcare providers, payors, and clearinghouses (*e.g.,* S. 3530,

the “Ensuring Patient Access to Healthcare Records Act”). While the Coalition agrees that Business Associates should be permitted to respond directly to individuals’ access requests and provide individuals with access to an aggregate view of information maintained by the Business Associate (when available), the Coalition does not believe that existing contract terms between clearinghouses, healthcare providers and health plans should be reversed or invalidated by the HIPAA Privacy Rule. The restrictions on healthcare clearinghouses in these contracts have been negotiated by healthcare providers and health plans to protect the PHI of patients and beneficiaries.

The Coalition also objected to the proposed legislation because it would have given healthcare clearinghouses special rights not afforded to other Covered Entities, such as granting healthcare clearinghouses a waiver from having to notify individuals directly in the event of a breach of unsecured PHI and the ability to charge individuals “fair market value” to respond to access requests. The Coalition continues to believe that healthcare clearinghouses should not be provided rights to use and disclose PHI beyond those given to other Business Associates because healthcare clearinghouses do not have a direct relationship with patients or beneficiaries and instead receive PHI on behalf of Covered Entities. Additionally, the Coalition does not believe that providing healthcare clearinghouses with special rights beyond those of other Business Associates would facilitate patients’ ability to receive accurate and complete PHI. Healthcare clearinghouses primarily handle billing and claims information, and do not have access to more meaningful clinical information such as test results or clinician notes. Further, a patient’s PHI often changes in the time following the healthcare clearinghouse’s processing of a claims transaction, and as a result, the information held by healthcare clearinghouses is not necessarily up to date or accurate.

The Coalition supports efforts to make it clearer to Covered Entities that they <u>may</u> disclose PHI to other Covered Entities for treatment, case management and care coordination purposes without first obtaining a HIPAA authorization.

In our members’ experience, many Covered Entities incorrectly require a requesting Covered Entity to obtain an authorization from the patient before they will send a medical record to another Covered Entity. This process frustrates patients. The Coalition believes, however, that this issue may be solved through education rather than a new regulatory requirement to disclose PHI to another Covered Entity when requested for treatment, case management, or care coordination purposes.

In addition, the Coalition believes that creating a requirement to disclose PHI for treatment, case management or care coordination purposes while providing patients an “opt-out” from such disclosures would create significant new administrative burdens for Covered Entities. Specifically, there would be significant costs in time and new technology to enable healthcare providers to present patients a choice to opt-out of sharing PHI, document opt-out requests in writing or in the healthcare provider’s EHR, and check the opt-out status before sharing any PHI for treatment, case management or care coordination purposes. HIPAA has long recognized that the seamless sharing of information for treatment, payment and healthcare operations is essential for the

efficient and safe delivery of healthcare – and this is even more acute in a value-based care environment. Granting patients a mandatory opt-out may prompt patients to prohibit routine data sharing without truly understanding consequences of opting out, and will frustrate, rather than enhance, the ability of Covered Entities to collaborate in value-based care arrangements.

A new regulatory requirement to disclose PHI when requested by Covered Entities or non-Covered Entity healthcare providers for treatment, case management or care coordination purposes could also create privacy risks. The current regulatory framework where treatment, payment, and healthcare operations disclosures are *permissible* rather than *required* allows the Covered Entity to exercise professional judgment in deciding whether the Covered Entity has received sufficient information (from the patient and the requestor) to determine that the request is legitimate and not from someone who does not in fact have a legitimate relationship with the patient. By making treatment, care coordination and case management disclosures *required*, Covered Entities may be forced to make the difficult decision of either violating the timing requirement for the new required disclosure, or violating HIPAA's requirement to adequately verify the identity of the requestor.

Additionally, should OCR propose to require the disclosure of PHI between Covered Entities, OCR should not require a Covered Entity to obtain an explicit affirmative authorization from the individual before initiating a request. Such a requirement would place an undue administrative burden on healthcare providers and might result in delayed treatment for the individual. A Covered Entity should be permitted to make a request for PHI from another Covered Entity based on the entity's professional judgement.

The Coalition also wishes to note that even if OCR provides additional guidance or promulgates a new regulation to require the disclosure of PHI between Covered Entities for treatment purposes, there are still more stringent state and federal laws (e.g., 42 C.F.R. Part 2) that would require the Covered Entity to obtain consent before disclosing PHI – even for treatment, case management or care coordination purposes. As discussed above, the Coalition supports modifying HIPAA to pre-empt state laws that are more stringent, as well as modifying incompatible federal laws, like 42 C.F.R. Part 2, to be more aligned with HIPAA's requirements.

The Coalition believes that if OCR elects to address the pathway for disclosing PHI to multi-disciplinary/multi-agency health and social services teams, it should do so through education and guidance rather than a change to the HIPAA Privacy Rule.

The Coalition agrees with OCR's assessment that Covered Entity healthcare providers are permitted to disclose PHI to multi-disciplinary/multi-agency teams without a patient's authorization under the "treatment" pathway. Some of our members are hesitant to make such disclosures, however, without first obtaining a consent or authorization from the patient. Multi-disciplinary/multi-agency teams are often not Covered Entities or Business Associates under HIPAA, and therefore the PHI would no longer be protected

by HIPAA's use and disclosure limitations following disclosure. As a result, some of our members will seek Business Associate-like assurances from multi-disciplinary/multi-agency teams before disclosing PHI to them when they are unable to obtain a HIPAA authorization or consent prior to the disclosure. Prior to making any change to the "treatment" definition, or developing an express pathway for disclosures to multi-disciplinary/multi-agency teams, the Coalition would encourage OCR to review best practices employed by Covered Entities for these disclosures. Such practices might involve obtaining some form of consent from individuals prior to these disclosures, or receiving written assurances from the multi-disciplinary/multi-agency team of the continued privacy of the PHI following such disclosures. OCR could then highlight best practices through education or guidance materials on these disclosures while leaving the current treatment pathway intact.

The Coalition believes that the applicability of the minimum necessary standard to case management and care coordination disclosures should not pose a barrier when Covered Entities and Business Associates are exercising good faith.

The Coalition believes that any perceived barriers created by the minimum necessary rule could be alleviated through guidance and education rather than a regulatory change. It may be helpful for OCR to provide further guidance on situations where it is permissible despite the minimum necessary requirement to provide Covered Entities and Business Associates with access to a full medical record for case management and care coordination purposes (in other words, where full access *is* the minimum necessary). For example, an ACO could potentially need access to the entire medical records of attributed patients to effectively conduct case management or care coordination. Based on OCR's previous guidance on using and disclosing entire medical records in FAQ 213,[1] we do not believe the minimum necessary standard would prevent such access. OCR could reiterate and supplement this FAQ guidance, however, by providing specific case management and care coordination scenarios where a Covered Entity would be justified in providing the patient's entire medical record.

We want to note that other state and federal laws could of course prevent a Covered Entity from providing the entire medical record for case management or care coordination purposes. For example, 42 C.F.R. Part 2 requires substance use disorder treatment programs and persons or entities that receive information from such programs to obtain a specific consent from the individual before they can use or disclose the protected substance use disorder treatment information for case management or care coordination. Although the Substance Abuse and Mental Health Services Administration ("SAMHSA") has made some modifications to the 42 C.F.R. Part 2 to enable health plans who receive substance use disorder information pursuant to a consent to re-disclose the information to their subcontractors for healthcare operations and payment purposes, SAMHSA has specifically excluded case management

[1] https://www.hhs.gov/hipaa/for-professionals/faq/213/what-conditions-may-health-care-provider-use-entire-medical-record/index.html

disclosures from this new pathway.[2] As a result, Covered Entities (including health plans) may need to exclude information protected by 42 C.F.R. Part 2 from case management or care coordination disclosures even if such information would normally be considered part of the "minimum necessary" information to perform such services.

These condition-specific laws likely create a greater barrier for case management and care coordination by the ACO than the minimum necessary rule. The Coalition continues to advocate for greater alignment between HIPAA and other federal and state laws governing the use and disclosure of medical records.

II. Promoting Parental and Caregiver Involvement and Addressing the Opioid Crisis and Serious Mental Illness

The Coalition believes that aligning non-preempted state and federal laws with HIPAA would allow Covered Entities to more readily share PHI with family members and others involved in the patient's care.

Under 42 C.F.R. Part 2, substance use disorder treatment programs and other holders of records protected by 42 C.F.R. Part 2 must obtain a specific written consent before disclosing information related to the patient's substance use disorder, including disclosures to family members and individuals involved in a patient's care. Similar state laws prevent providers who treat serious mental illness from disclosing information to family members or others without the patient's written consent. These non-HIPAA consent requirements create a significant barrier for healthcare providers that treat patients with opioid dependence or severe mental illness to share information with family members, friends, adult children of parents, or others.

Unlike more stringent federal and state laws, HIPAA permits healthcare providers to disclose PHI to family members and others involved in the patient's care, provided the patient has had the opportunity to agree or object to the disclosure. Where 42 C.F.R. Part 2 or more stringent state laws governing information related to mental illness do not apply, this pathway gives healthcare providers significant discretion in cases where a patient is incapacitated or not present to agree or object to such disclosures.

Rather than alter the personal representative pathway, OCR could consider providing guidance on a patient's opportunity to agree or object to disclosures of PHI to family members, friends, or others involved in their care. Through guidance, OCR could assure healthcare providers that they may disclose PHI to family members, caregivers and others to promote health and recovery when the individual does not object, or in the healthcare provider's professional judgment, is not capable of agreeing or objecting to the disclosure due to the effects of substance use disorder or severe mental illness.

III. Accounting of Disclosures

[2] 83 Fed. Reg. 239, 243-244 (Jan. 3, 2018).

The Coalition commends OCR for indicating that it will not finalize the 2011 Proposed Rule that would have expanded the accounting of disclosures requirement. The Coalition encourages OCR to assess whether consumer demand and technology support any expansion of the accounting of disclosures requirement given the provision in the HITECH Act that requires the Secretary to weigh "the interests of the individuals in learning the circumstances under which their protected health information is being disclosed and…the administrative burden of accounting for such disclosures."[3]

We thank OCR for announcing its intention to remove the May 2011 Accounting of Disclosures proposed rule that would have created a new right for patients to receive an "access report" that tracked accesses to PHI maintained in an electronic health record (EHR). As the Coalition noted in its comments to that proposed rule, we felt the access report proposal was overly burdensome to Covered Entities, and unworkable with currently available technology. Further, the Coalition does not believe that EHR technology has yet reached a point where it could capture and integrate into a single, human-understandable format all disclosures for treatment, payment, and healthcare operations. To our knowledge, EHRs do not have the capability to capture and maintain information about all treatment, payment, and healthcare operations disclosures, and cannot distinguish between "uses" and "disclosures" through the EHR. Even if the systems collected the required information, running such audits would take a material amount of time, and the EHR would not necessarily be able to display the results in a user-friendly format. Significant worker-hours would potentially be needed to manually sort through the information to make it usable.

Indeed, preparation of accounting of disclosures reports today (for non-routine disclosures) requires significant manual effort, including chart review and searches of spreadsheets received from various departments that are used by Covered Entities to make disclosures required by law, such as for communicable disease reporting. OCR should be cautious about establishing an expanded accounting of disclosures requirement that would increase healthcare providers' costs significantly without providing a true benefit to patients.

Last year, we performed a survey of our members to determine how often they receive requests for an accounting of disclosures. Based on our members' experience, patients are not frequently requesting an accounting. To illustrate, one health system has received only 25 such requests over a 14-year period. Requiring Covered Entities to adopt special, expensive technology – that to our knowledge is yet to be developed, and is not required to be offered by EHR developers in the most recent edition of certified EHR technology— to be able to accommodate a very small number of requests does not seem to fit into OCR's and HHS's overall goal of removing regulatory obstacles and decreasing regulatory burdens in order to facilitate efficient care coordination and case management. The Coalition similarly believes that requiring Covered Entities to account for their *Business Associates'* disclosures for treatment, payment or healthcare

[3] 42 U.S.C. § 17935

operations, or for Covered Entities to forward on such requests to their Business Associates would simply add costs and complexity to the system for negligible patient benefit.

Importantly, patients who do ask for an accounting of disclosures under current law often reverse course when they are told what an accounting of disclosures report would contain. Instead, what these patients typically are seeking is an investigation into whether a specific user of the EHR inappropriately viewed their record. Rather than modify the accounting of disclosures provision at 45 C.F.R. § 164.528, the Coalition recommends that OCR consider providing guidance on 45 C.F.R. § 164.530(d), which describes how a Covered Entity develops policies and procedures to effectively respond to complaints. Covered Entities' policies and procedures concerning patient complaints could, for example, address how the Covered Entity responds to situations where patients express concern about the potential inappropriate use or disclosure of PHI in their electronic health record.

The Coalition notes, however, that any such policies and procedures and the investigations carried out by Covered Entities in response to patient complaints should be evaluated by OCR in accordance with the congressionally-mandated balancing test, which calls for the Secretary to "only require such information to be collected through an electronic health record in a manner that takes into account the interests of the individuals in learning the circumstances under which their protected health information is being disclosed and takes into account the administrative burden of accounting for such disclosures."

Many Covered Entities already spend significant time investigating individuals' concerns that a specific user *inappropriately* accessed or disclosed their PHI. These investigations can require the Covered Entity to employ a variety of techniques and processes. One large health system that typically investigates over 100 patient privacy complaints or concerns each year uses security audit logs and data correlation tools to identify potentially inappropriate access, and then conducts in-person interviews to understand the purpose of each questionable access of the patient's PHI. Based on this health system's experience, patients are, with very rare exception, satisfied with these privacy investigations.

Importantly, while we would support informing individuals about privacy investigation outcomes in a general sense, we do not believe that employee names or human resources-related actions should necessarily be provided to the individual. We also note that if inappropriate access is identified as a part of an investigation request, the subsequent breach notifications required under the Breach Notification Rule provide important information to individuals about the nature of the incident and steps the individuals can take to protect their privacy. The Breach Notification Rule does not require the Covered Entity to include the name of the person or persons who accessed the individual's PHI inappropriately, however.

IV. Notice of Privacy Practices

The Coalition supports the removal of the requirement for healthcare providers to obtain an acknowledgement from patients of their receipt of the Notice of Privacy Practices upon the patient's first visit, and supports efforts by the Office for Civil Rights to make the notice more understandable and meaningful to consumers.

The Coalition commends OCR for proposing in the RFI the removal of the requirement for Covered Entity healthcare providers to obtain an acknowledgment from patients of their receipt of the Covered Entity's Notice of Privacy Practices. In addition to alleviating the number of signatures that a healthcare provider must require the patient to provide during intake process, the removal of the acknowledgment requirement would also help to alleviate document retention burdens placed on Covered Entities under the HIPAA Privacy Rule. In particular, our members noted that retaining signed acknowledgments of the Notice of Privacy Practices for six years creates significant storage costs. In our view, the value of having the individual acknowledge receipt of the Notice is outweighed by the burdens associated with the requirement.

The Coalition agrees with OCR's observation that some patients may not fully read or understand the contents of healthcare providers' and health plans' Notice of Privacy Practices, and supports efforts by OCR to simplify the Notice requirement. We note, however, that while the HIPAA Model Notice provides an easy-to-understand overview of patients' rights and permitted and required disclosures of PHI, the general format of the implementation specifications for the HIPAA Notice of Privacy Practices does not encourage differentiation between healthcare providers' and health plans' Notices of Privacy Practices. As a result, the role of the Notice acts more as an explanation to the patient or beneficiary of HIPAA's protections and potential disclosures rather than a description of how the healthcare provider or health plan actually uses or disclosures.

We do not offer this observation to suggest that OCR change the Notice's implementation specifications. Rather, we offer this observation as support to OCR's decision to remove the requirement to obtain an acknowledgment of receipt of the Notice, and to instead focus on other ways healthcare providers, health plans, and OCR itself can help make individuals more aware of how HIPAA protects their PHI.

V. Additional Ways to Remove Regulatory Obstacles and Reduce Regulatory Burdens to Facilitate Care Coordination and Promote Value-Based Health Care Transformation

The Coalition encourages OCR to review potential regulatory burdens in the Security Rule (in addition to the Privacy Rule) that may be inhibiting the exchange of PHI for care coordination, case management, and value-based payment programs. Currently, there is significant confusion concerning the requirements for conducting a risk analysis and mitigating identified risks. This confusion impacts the disclosure of PHI for case management and care coordination because Covered Entities and Business Associates are reluctant to disclose PHI to entities that are either not subject to the HIPAA Security Rule requirements, or do not appear to be sufficiently aware of them. The Coalition would welcome additional guidance or safe harbors for compliance with the HIPAA Security Rule so that Covered Entities and their Business Associates can have better

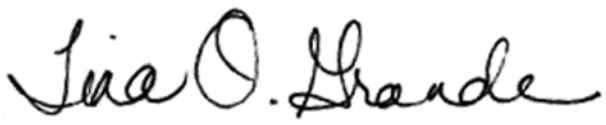
assurance that they (and their recipients) are meeting OCR's expectations from a security perspective.

The Coalition similarly would like OCR to consider a compliance safe harbor for organizations that meet OCR guidance in establishing a security program, but nonetheless become a victim of a cyber-attack. There is currently a lack of clarity on the level of risk Covered Entities are exposing themselves to when disclosing PHI to other systems/organizations through tools like health information exchanges and how much diligence they need to conduct on these systems/organizations to avoid OCR enforcement if an attacker gains access.

VI. Conclusion

The Confidentiality Coalition appreciates this opportunity to provide comments on the HIPAA RFI. Please contact me at tgrande@hlc.org or at (202) 449-3433 if there are any comments or questions about the comments in this letter.

Sincerely,



Tina Grande

Enclosures

APPENDIX A

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.

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
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
LEO Pharma
Mallinckrodt Pharmaceuticals
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
Stryker
Surescripts
Teladoc
Texas Health Resources
UCB
UnitedHealth Group
Vizient
Workgroup for Electronic Data Interchange
ZS Associates

CONFIDENTIALITY COALITION

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.

Revised January 2019