CONFIDENTIALITY COALITION

Advancing Health Care. Safeguarding Trust.

SUBMITTED ELECTRONICALLY

June 3, 2019

Centers for Medicare & Medicaid Services
Department of Health and Human Services
7500 Security Boulevard
Baltimore, MD 21244–1850

RE: Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans in the Federally-Facilitated Exchanges and Health Care Providers (CMS–9115–P)

Dear Sir or Madam:

The Confidentiality Coalition (the Coalition) respectfully submits these comments in response to the Centers for Medicare & Medicaid Services' (CMS) proposed rule to advance interoperability and patient access to health information (the Proposed Rule). We also want to thank CMS for graciously extending commenters additional time to review and comment on the Proposed Rule given its complexity.

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.

We have attached additional information about the Coalition and its membership as Appendix A. Given the Coalition's focus on policies and practices affecting the privacy and security of patient information, we have focused our comments below on CMS's proposal to require certain CMS-regulated health plans to adopt Application

Programming Interfaces (APIs), and requests for comment on patient matching and trusted exchange.

COMMENTS

Application Programming Interfaces

The Coalition generally supports CMS's proposal to bring the functionality of HL7's Fast Healthcare Interoperability Resources (FHIR)-based APIs to Medicare Advantage (MA) plans, Medicaid state agencies, Medicaid managed care plans, Children's Health Insurance Program (CHIP) agencies, CHIP Managed Care entities, and issuers of qualified health plans (QHPs) in Federally-Facilitated Exchanges (FFEs) (Covered Plans and Agencies). We are concerned, however, that Covered Plans and Agencies will not have sufficient time under the Proposed Rule to implement this mandate. Under the proposal, Covered Plans and Agencies must implement an API by January 1, 2020 for MA plans and QHP issuers in FFEs, and by July 1, 2020 for Medicaid FFS, Medicaid managed care plans and CHIP managed care entities. With this Proposed Rule and the Office of the National Coordinator for Health Information Technology's 21st Century Cures proposed rule unlikely to be finalized until later this year (at the earliest), we believe it is unrealistic to expect Covered Plans and Agencies to adopt FHIR-based APIs so quickly. We urge CMS to give Covered Plans and Agencies sufficient time to develop and test their APIs, and ensure the security of the connections they are establishing. Additionally, any new interoperability requirements should follow – not precede – regulation of any and all applications that receive electronic health information (EHI).

While we are excited about the possibilities that FHIR-based APIs can unlock for plan members, we want to raise important privacy and security concerns related to using the API to provide access to third party applications of an individual's choice. While the Coalition supports efforts to make it easier for members to obtain access to their health information electronically, third party applications selected by plan members are not consistently subject to the Health Information Portability and Accountability Act's (HIPAA) Privacy and Security Rules because many of these applications are not offered by or on behalf of covered entities, but are rather offered as direct to consumer services. Many individuals do not fully appreciate that the protections of HIPAA do not extend to these applications. We are concerned that individuals will not have enough information to be educated consumers, and that they may not understand that they are assuming the risk of the security practices by their chosen application. While we thank the Office for Civil Rights (OCR) for recently released guidance clarifying that healthcare providers and health plans are not responsible under the HIPAA Security Rule for verifying the security of a patient or member's chosen third party application, this "safe harbor" does not address the potential vulnerability of individuals' health information when sent to the application.

We propose that CMS, ONC, the Federal Trade Commission (FTC) and OCR develop or recognize existing private sector privacy and security trust or certification frameworks

that could be used to assess third party applications seeking to connect to APIs of healthcare providers and health plans. Such programs could foster innovation, while providing better assurance to individuals of the privacy and security of their health information. CMS, ONC and OCR should establish safe harbor provisions that allow and encourage healthcare organizations to share threat information about security risks and incidents linked to third-party applications.

Policies to Improve Patient Matching

The Coalition supports private sector efforts to improve patient matching algorithms and standardize data elements, as well as private sector efforts to develop unique patient identifiers (UPIs) to improve accuracy of patient matching. In particular, we encourage CMS to support the standardization of patient demographic data by, for example, applying the U.S. Postal Service Standard to addresses.

The Pew Research Center (Pew) recently collaborated with Indiana University to test whether standardizing demographic fields (including address, phone number, name, and others) would yield improvements to patient matching. To conduct the research, Indiana University ran a matching algorithm across four different databases where the true matches were already known. Pew then standardized the data and re-ran the algorithm to determine whether standardization generated better matching results. The research indicated that use of the U.S. Postal Service standard for addresses can increase match rates by approximately 2-3 percent—which would make a meaningful difference. Standardizing last name alongside address showed further improvement in match rates (up to approximately 8 percent).

CMS requested information on whether to require program participants to use a patient matching algorithm or a solution with “proven” success validated by the Department of Health and Human Services (HHS) or a third party. The Coalition recommends that CMS examine how to benchmark different approaches to patient matching, measure the variation across matching algorithms and highlight current limitations. Benchmarking on its own, however, will not improve match rates. CMS should work with ONC to optimize the use of demographic data (including adoption of the U.S. Postal Service standard for addresses and the use of additional data elements).

CMS also requested information on whether to expand recent Medicare ID card efforts by requiring a CMS-wide identifier for all beneficiaries and enrollees in healthcare programs under its administration and authority. Implementing an agency-wide identifier may help CMS better serve beneficiaries and improve matching. This approach, however, is still insufficient to address patient matching on a nationwide scale.

Finally, CMS requests information on whether it should advance more standardized data elements across all appropriate programs for matching purposes by perhaps leveraging the U.S. Core Data for Interoperability (USCDI) proposed by ONC. We

support the proposed inclusion of address in the USCDI, and again encourage CMS to work with ONC to advance the use of the U.S. Postal Service standard for addresses.

Trusted Exchange Network Requirements for MA Plans, Medicaid Managed Care Plans, CHIP Managed Care Entities, QHPs in the FFEs, and Innovation Center Models

The Coalition believes it is premature for CMS to require participation by plans and innovation center models in trusted exchange networks. The second version of the Trusted Exchange Framework and Common Agreement (TEFCA) was just released for comment on April 19, 2019 – over a month after CMS and ONC published the NPRMs in the Federal Register. We believe CMS and ONC should give stakeholders more time to digest and comment on the revisions made to the TEFCA framework before seeking feedback on the criteria proposed by CMS for a "trusted exchange network."

For example, the Coalition is concerned with the way TEFCA proposes to treat sensitive data – requiring security metadata labeling for four types of data without taking into account the reality of differing state law approaches. The metadata tagging required under the ONC proposal could result in insufficient information being tagged in some states, and too much information tagged in other states. The Coalition has long held that physicians need access to all of a patient's information to provide safe and effective care. The Coalition recommends that CMS and ONC encourage further discussion among state governors to harmonize state privacy laws concerning health information, which would greatly improve trusted exchange amongst health plans and healthcare providers.

The January 1, 2020 deadline for compliance with this trusted exchange network requirement is far too aggressive. We recommend that CMS postpone this requirement until at least January 1, 2021, and delay enforcement until January 1, 2022 at the earliest.

Proposed Compliance Deadlines

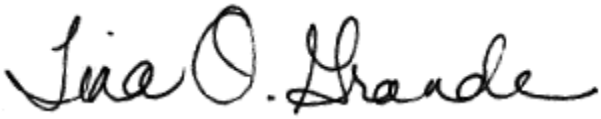
CMS and ONC have issued proposed rules that are interdependent and require sequential implementation of new requirements between them. The timeframes for adoption of new requirements, testing and implementation in the Proposed Rule exceed the deadlines for compliance in the companion ONC rule. Misaligned compliance dates between the two rules will undermine adoption and implementation efforts. We strongly

recommend that CMS set compliance dates that are the same as ONC's, and in any case no less than 24 months after the Final Rules are published.

Conclusion

The Confidentiality Coalition appreciates this opportunity to provide comments to CMS on the Proposed Rule. 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 O. Grande
Chair, Confidentiality Coalition and
Senior VP, Policy, Healthcare Leadership Council

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
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

Revised May 2019

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