CONFIDENTIALITY COALITION

Advancing Health Care. Safeguarding Trust.

SUBMITTED ELECTRONICALLY

June 3, 2019

Office of the National Coordinator for Health Information Technology
Mary E. Switzer Building
330 C Street SW
Washington, DC 20201

RE: 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program (RIN 0955–AA01)

Dear Sir or Madam:

The Confidentiality Coalition (the Coalition) respectfully submits these comments in response to the Office of the National Coordinator for Health Information Technology (ONC) proposed rule to implement changes under the authority of the 21st Century Cures Act (the Proposed Rule). We also want to thank ONC 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 the privacy and security implications of the Proposed Rule.

COMMENTS

Information Blocking Provisions

The Coalition supports Congress's and the Administration's efforts to eliminate information blocking to ensure that patients have facilitated access to information about their healthcare, and that healthcare providers may effectively use and exchange health information with third parties in accordance with the Health Insurance Portability and Accountability Act (HIPAA) and other federal and state laws. We note, however, that the information blocking provisions in the 21st Century Cures Act are not meant to override HIPAA or other federal and state laws, but rather are meant to work within that structure. Against that backdrop, the Coalition is concerned that the Proposed Rule may apply the information blocking prohibition too broadly, and establish privacy and security exceptions to information blocking too narrowly, inadvertently creating inconsistencies with requirements of HIPAA and other federal and state laws, and forcing healthcare providers, developers of certified health IT, health information networks, and health information exchanges (Actors) to choose between violating the information blocking restrictions, which could result in significant penalties, or violating other federal or state laws that limit the sharing of individually identifiable health information (IIHI). As a result, we believe there is a risk that Actors will feel compelled to share *too much* health information, at the potential detriment to the privacy and security of IIHI. Below, we provide our comments on the information blocking provisions in the Proposed Rule.

Definition of Electronic Health Information

ONC proposes to define the term "electronic health information" or "EHI" to include electronic protected health information (PHI) (as defined by HIPAA) and any other electronic information that identifies an individual and relates to the past, present or future health or condition of an individual, the provision of healthcare to an individual, or the past, present or future payment for the provision of healthcare to an individual.

First, the Coalition applauds ONC for excluding de-identified data in the definition of EHI. We believe that Congress's focus in the 21st Century Cures Act was to encourage the flow of identifiable *clinical information* between systems – not to affect, and potentially discourage, the creation or application of de-identified data. It takes significant time and resources for Actors to develop databases of de-identified data for research, quality improvement and quality assurance purposes. Requiring Actors to make the data in these databases widely available to third parties under the fee constraints established by the Proposed Rule would inhibit innovation and potentially jeopardize the de-identified nature of the information given the wider audience and potential for unconstrained secondary use of the data.

We recommend that ONC further narrow the definition of EHI in the final rule. As the definition of EHI plays an important role in determining whether an activity triggers information blocking restrictions or conditions of certification requirements, the breadth of this definition as currently proposed could lead to the following unintended results:

- If a developer of certified health IT elects to develop and offer appointment scheduling/practice management software *separate* from its certified health IT, the developer would be subject to the information blocking restrictions with respect to both its electronic health record *and* the appointment scheduling/practice management software. Meanwhile, an entity that does not have a certified health IT product may create appointment scheduling/practice management software and would not be subject to the information blocking restrictions. There is no public benefit to treating two otherwise similar appointment scheduling/practice management software offerings differently.

- If a health IT developer of certified health IT "produces and electronically manages" EHI, the health IT developer may under the proposed rule be required to develop and obtain certification for an "EHI Export" mechanism, even if the EHI is "produced or electronically managed" in a separate registry or database from the health IT developer's certified health IT. This means, for example, that if the health IT developer wanted to develop a health IT solution separate and apart from its certified health IT to permit a patient safety organization to collect and track case reports, the developer would potentially need to obtain certification from an ONC-approved certification body to ensure the product contained certified EHI export functionality.

In order to avoid these and other unintended consequences of such a broad definition for EHI, we recommend that ONC limit the definition to IIHI *maintained electronically in a designated record set*. Constraining EHI to IIHI maintained electronically within a designated record set would better capture the universe of IIHI that Congress sought to protect in the 21st Century Cures Act, specifically, *clinical information* which is maintained within electronic health record and claims management systems, and needed by healthcare providers and health plans to make treatment and payment decisions about individuals.

Privacy Exception

The Coalition agrees with ONC's inclusion of an exception to information blocking that recognizes Actors' interest in maintaining the privacy of IIHI and complying with HIPAA and state privacy laws. We are concerned, however, that given the limited nature of the sub-exceptions and stringent documentation requirements for meeting them that Actors will be understandably concerned about inadvertently triggering a penalty. To avoid doing so, Actors may be unintentionally incentivized to *overshare* EHI *without* satisfying privacy-protective pre-conditions established by HIPAA and other laws, such as the verification requirements at 45 C.F.R. § 164.514(h). As we note above, the information

blocking provisions from the 21st Century Cures Act were not intended to override HIPAA or other federal and state laws, and therefore providers must be affirmatively permitted to comply with HIPAA. We recommend that ONC clarify in the final rule that Actors do not face penalties under the information blocking provisions when they elect to not disclose information in a good faith effort to comply with HIPAA and state privacy laws. We also ask ONC to specifically clarify that a business associate following provisions of a business associate agreement that restricts data sharing (and thereby allows a covered entity to follow and comply with its privacy policy) would not be subject to penalties for following those instructions. We note that covered entities hold the relationship with the consumer/patient, and business associates must be able to follow covered entities' posted privacy policies, including directing how and where patients may access their IIHI.

Additionally, the Coalition requests that ONC extend the HIPAA provisions that allow covered entities and business associates to decline to disclose information when that information is part of active research (particularly for masked or blinded research designs) to all Actors. Data held for research may be part of a masked or blinded study, may be a limited data set and/or will not contain identifiers in compliance with minimum necessary standards (HIPAA Privacy Rule methods to protect privacy), that would make it infeasible to share information. Research organizations are not covered entities or business associates, but are likely to meet the definition of a Health Information Network. This is another example of what is likely unintended oversharing that could be addressed by specifically extending permission to not share EHI collected and used for research during the active study using a blinded or masked research design.

While it is possible that some Actors may inappropriately seek to use privacy laws as a shield against disclosing EHI, the requirement that Actors decline disclosures only in good faith should significantly reduce this possibility, such that it is outweighed by the gained privacy and security protections for individuals by broadening the privacy exception.

As currently defined in the Proposed Rule, the privacy exception would require significant administrative complexity to implement. For example, in order to meet the "pre-condition not satisfied" sub-exception, the Actor not only needs to have written policies and procedures in place concerning the federal or state privacy pre-condition, but must also do "all things reasonably necessary within its control to provide the individual with a meaningful opportunity to provide" a consent or authorization to share the information.

The Coalition believes that when a third party application is acting on behalf of an individual to request EHI from an Actor, ONC should permit the Actor to require that the third party obtain the necessary consent or authorization to satisfy the privacy pre-condition. For other use cases, we believe that Actors should also be permitted to decide that it would be too burdensome to seek multiple consents or authorizations to share IIHI at the request of a third party. For example, if a case management service

requests access to EHI pertaining to multiple patients' substance use disorder treatment, the healthcare provider should not be penalized for deciding that it would be too difficult to seek consent or authorization from each applicable patient to share EHI with the case management service provider.

The Coalition believes that the key to unlocking information protected by state or federal laws that are more stringent than HIPAA is to harmonize state and federal laws to the HIPAA standard – thereby removing any preconditions to sharing the information for treatment, payment and healthcare operations purposes. Penalizing Actors for not engaging in "all things reasonably necessary within its control" to obtain consents or authorizations only stands to further aggravate the burdensome nature of more stringent privacy laws.

Given the existing patchwork of state privacy laws, however, the Coalition encourages ONC to adapt its proposal to permit Actors who operate across multiple states to implement the pre-conditions of state laws that are the most stringent for purposes of this sub-exception. It is often too difficult for organizations operating across state lines to develop different consent workflows for each state, and ONC is right to recognize that organizations instead will implement the most stringent state law. As long as Actors implement a state-mandated pre-condition consistently when responding to requests, we believe Actors should be permitted to select which portions of a state law to implement globally across states rather than being required to provide "all privacy protections afforded by that law across its entire business." It may be impossible to implement some aspects of a state law, such as data retention requirements, across state lines without violating the laws of another state. As a result, we believe ONC should give Actors leeway to select which state law requirements they wish to apply globally as opposed to just the residents of the applicable state.

Security Exception

Security threats to EHI are constantly increasing, and any organization that transmits EHI must continue to exercise vigilance to ensure the security of the transmission. For this reason, the Coalition applauds ONC for establishing an exception to the information blocking prohibition when an Actor denies access to information due to a tailored, non-discriminately implemented security practice directly related to safeguarding the confidentiality, integrity and availability of EHI.

The Coalition also appreciates that ONC provides two methods of denying access, exchange or use of EHI on security grounds: 1) on the basis of a written organizational security policy; or 2) on a case-by-case, facts and circumstances basis when the security practice is necessary to mitigate the security risk to EHI, and there are no reasonable and appropriate alternatives to the practice that are less likely to interfere with the access, exchange or use of EHI. While organizational security policies and procedures often provide strong processes for evaluating and mitigating risks, it can be difficult in a written organizational policy and procedure to address specific parameters for establishing differing levels of access to various systems that contain EHI. As a

result, it is helpful that ONC has provided Actors an option to evaluate requests on a case-by-case basis to address potential security risks in a reasonable and appropriate manner.

As we discuss in further detail in the section below, we believe ONC should clarify in the final rule that Actors may apply the steps established by this security exception when "verifying" third party application developers prior to permitting them to connect to Application Programming Interfaces (APIs).

Application Programming Interfaces

The Proposed Rule would require developers of certified health IT to share EHI with third party applications of a patient's choice through new, innovative APIs that utilize the Fast Healthcare Interoperability Resources (FHIR) protocol. These third party application developers, which are entering the healthcare market at a rapid pace, are often not covered by HIPAA because they offer their applications directly to consumers and not on behalf of a covered entity healthcare provider or health plan. The Coalition asks ONC and the Department of Health and Human Services (HHS) to take additional steps to ensure a thoughtful approach to how Actors, many of whom are covered by HIPAA as covered entities or business associates, share EHI with these non-HIPAA entities, and ensure that such third party applications are equipped to handle IIHI.

HIPAA Considerations

We are concerned that patients 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. Consumers do not necessarily understand when their IIHI is and is not protected by HIPAA. While we appreciate the Office for Civil Rights' (OCR) recently released guidance clarifying that healthcare providers are not responsible under the HIPAA Security Rule for verifying the security of a patient's chosen third party application, this "safe harbor" does not address the potential vulnerability of patients' IIHI when sent to the application.

According to the Proposed Rule, an Actor cannot conduct "verification" checks on individual third party applications before allowing the application to connect to its API, but rather must conduct such "verification" on the developers themselves, and must complete the process within five business days. Although ONC provides some examples of acceptable "verification" processes in the Proposed Rule, the permissible scope and purpose of "verification" is still unclear given that the Actor is not permitted to seek additional information about the third party developer's application or its security readiness. We ask that ONC provide further guidance on the types of "verification" that will be permitted, and that it consider permitting Actors to undertake some form of review of third party applications themselves before permitting them to connect to their APIs.

We propose that ONC and/or OCR work with the private sector to develop a privacy and security trust or certification framework for third party applications seeking to connect to APIs of certified health IT. Once established, ONC should permit developers of certified health IT and healthcare providers to limit the use of their APIs to third party applications that have agreed to abide by the framework. Such a program would foster innovation, while providing better assurance to patients of the security of their IIHI – even if they are not aware of when HIPAA applies.

Oversight of Third Party Applications to Reduce Privacy Risks to Consumers

We strongly encourage ONC and CMS to recognize existing private sector voluntary certification programs and/or shepherd the development of new voluntary certification programs that assess the privacy and security of a business's systems. This would help the agencies exercise oversight over third party products and vendors offering consumer services for accessing information obtained from HIPAA covered entities, health IT developers, Health Information Networks or Health Information Exchanges. We recommend both agencies consider establishing a public registry to report apps or services that have violated (or are reasonably suspected of violating) their terms of use or that have credibly threatened cyber security, e.g., through malware injection. ONC should provide Actors an enforcement safe harbor from information blocking claims to allow Actors to deny access to registry-listed third parties. ONC should support the Federal Trade Commission (FTC) in regulating entities subject to FTC authority, including notice requirements informing consumers of their rights and remedies.

Population-Level Queries

ONC also requires certified developers of health IT that are seeking certification under the API criterion to demonstrate functionality that would allow an organization (such as a case management vendor for a health plan) to query and receive data from the API concerning multiple patients. Given that there is not yet a consistent, standardized specification for FHIR servers to handle searches for multiple patients, ONC clarified that the developer may approach searches for multiple patients in the manner it deems most efficient to meet this proposed certification criterion.

We are concerned that the current lack of a standard for implementing population-level queries could result in implementation of solutions that raise privacy concerns. In particular, we worry that certified health IT developers will implement different methodologies of varying maturity to match patients within the certified health IT to the patients listed in the population-level query. Each incorrect patient match represents a potential breach of PHI, which could expose the healthcare provider implementing the API to potential liability under HIPAA.

We ask that ONC clarify that healthcare providers who choose not to implement the population-based query functionality would not be engaged in information blocking. We also ask that ONC clarify that healthcare providers that do elect to implement population-based queries have leeway under the privacy and security exceptions to

information blocking to deny population-level queries if there would be issues in matching patients within the system to the list of individuals that the querying party requested, or other security concerns.

Privacy and Security Transparency Attestations Criteria

ONC proposes two new privacy and security attestation requirements on developers of certified health IT that would indicate whether the certified health IT supports encrypting authentication credentials and/or multi-factor authentication. The Coalition believes that certification to these required attestations will increase transparency and potentially motivate health IT developers to encrypt authentication credentials and support multi-factor authentication.

The Coalition notes that under HIPAA, covered entities and business associates may evaluate whether it is reasonable and appropriate to implement both encryption of authentication credentials and multi-factor authentication. We ask ONC to clarify that its decision to list these attestations on the Certified Health IT Product List does not create new requirements for healthcare providers to implement multi-factor authentication or encryption of user credentials unless their security risk analysis determines that the implementation of these safeguards is reasonable and appropriate to mitigate potential risk.

Data Segmentation for Privacy and Consent Management Certification Criteria

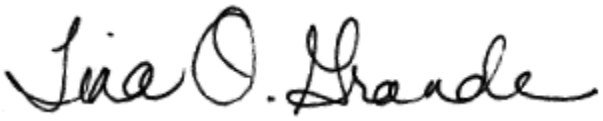
In the Proposed Rule, ONC proposes to modify the Data Segmentation for Privacy certification criterion to permit metadata tagging at the section and entry level. We are concerned with this proposed granular approach to data tagging for health information exchange. Specifically, the Coalition is concerned that the proposed metadata tagging tools are not yet mature enough for release. In the Proposed Rule, ONC references studies and publications, but we believe these are insufficient to justify the proposed wide-scale implementation of data segmentation tools. Currently metadata tagging is accomplished at the document level, e.g., an entire Consolidated-Clinical Document Architecture document. In the absence of a mature market for advanced automation tools, metadata tagging at more detailed levels would be unduly burdensome for providers.

The Coalition has long held that physicians need access to all of a patient's information to provide safe and effective care. Records that contain gaps or redactions could potentially be harmful to patient safety. We believe that HHS should look for ways to harmonize state and federal privacy policies so that providers can share all PHI as needed for treatment. We believe that all of us need to undertake efforts to lessen the stigma associated with so-called "sensitive" health conditions rather than proliferating any continued sense of stigma by labelling data as sensitive through data segmentation.

Conclusion

The Confidentiality Coalition appreciates this opportunity to provide comments to ONC 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