

June 24, 2019

Hon. Alex Azar II  
United States Secretary of Health & Human Services  
200 Independence Ave SW, Room 600  
Washington, DC 20201

Re: Comment to Proposed Rule  
ONC Information Blocking Regulation (RIN 0955-AA01)

Dear Secretary Azar:

The Healthcare and Public Health Sector Coordinating Council (HSCC) Cybersecurity Working Group (CWG) is pleased to comment on the Office of the National Coordinator for Health Information Technology's (ONC) proposed rule, "21<sup>st</sup> Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program," published in the *Federal Register* (84 FR 7424) on March 4, 2019.

The HSCC is a private sector-led advisory council of major health industry stakeholders working together and with the U.S Department of Health & Human Services (HHS) to identify and mitigate threats and vulnerabilities affecting the ability of the sector to deliver healthcare services to the nation's citizens. A major component of the HSCC is its Cybersecurity Working Group, which represents more than 200 healthcare organizations in the subsectors of direct patient care, medical materials, health information technology (health IT), health plans and payers, laboratories, biologics and pharmaceuticals, and public health. Our members collaborate toward improving the cyber security and resiliency of the healthcare industry and patient safety.

### Comments

#### **Section IV- Updates to the 2015 Edition Certification Criteria**

ONC is proposing a 24-month development timeline for most of its proposed certification changes. ONC is also proposing to adjust the definition of 2015 Edition Base EHR to comport with ONC's certification requirements within 24 months of the final rule's effective date. Our industry is very supportive of advancing widespread interoperability such that technology supports clinicians and ultimately the patients they serve. Because most providers are bound to the use of 2015 Edition Base EHRs through CMS program requirements, **as proposed, the 24-month timeline would require EHR vendor development and provider EHR adoption, implementation, and use concurrently.** We are concerned that this timeline is not practical and will have a negative impact on the security of information systems using electronic health record systems (EHRs). There are some providers who worry that a rushed timeline will create patient safety challenges. We need a sufficient, realistic timeline for health IT developers and vendors to produce well designed and thoroughly tested modifications to meet the requirements for certification of EHR technology. As this work moves forward, we believe it is important that the progress our industry is making is adequately measured.

In addition, healthcare providers and facilities required to attest to the use of certified electronic health record technology (CEHRT) employing the revised 2015 Edition Criteria will need sufficient time to procure, update, install or test the changed CEHRT prior to placing the system into production. **For these reasons, and to prevent significant confusion for providers about program requirements, we strongly recommend that ONC refrain from adjusting the 2015 Edition Base EHR definition.** Further, we do not agree with ONC’s rationale to avoid proposing a new Certified Health IT Edition designation. The proposed modifications to 2015 Edition CEHRT will make substantive changes to EHR design, functionality, use, and performance. ONC should release a new Edition. **We recommend that ONC adopt a 2020 Edition or the corresponding year in which this rule is effective.** HHS should direct its agencies to update regulations to reflect the new Edition. As this work moves forward, we believe it is important that the progress our industry is making is adequately measured.

### **§170.315(d)(13) Multi-factor authentication**

We are pleased to see that HHS has proposed to update the 2015 Edition of its Health IT Certification Criteria to reflect the importance of Multi Factor Authentication (MFA) in the health sector. As HHS notes in the proposed rule, *“Using a single factor approach to accessing information is particularly prone to cyber-attack because one factor passwords can be weak, stolen, and are vulnerable to external phishing attacks, malware, and social engineering threats.”* HHS’s proposed approach of requiring vendors to publicly disclose whether they are supporting MFA should help create significant market pressure to drive all vendors in that direction. However, before HHS stipulates a mandate on vendors for inclusion of MFA, there must be an opportunity for stakeholders to comment on what the MFA standards will be.

Nonetheless, we have some recommendations for improving this language. We recommend HHS:

1. Require vendors to explain how they are supporting MFA. As the National Institute of Standards and Technology (NIST) has indicated in its Digital Identity Guidelines (SP 800-63-3), all MFA is not the same. MFA based on technology like SMS has proven to be vulnerable to phishing attacks, as well as SIM-swap attacks and attacks on the SS7 protocol. Likewise, token or app-based One-Time Password (OTP) MFA solutions have also proven to be “phishable,” given that they are based on shared secrets. These technologies are still recognized in SP 800-63-3 but are not classified as being as strong as other types of authentication technologies. Given the wide variation in the security of different types of MFA – and the risks inherent with using some legacy MFA technologies (see the Preamble to the Proposed Rule at page 7451) – we believe that vendors should be required to provide details outlining specifically which MFA technologies they are supporting . If one goal of this new rule is to “provide more public transparency around the MFA capabilities included in certified health IT,” then requiring these additional details would increase transparency.
2. Create a publicly available website where all vendor disclosures are published and can easily be indexed and searched. This would make it much easier for any purchasers of health IT solutions to understand whether different vendors implement MFA and how they implement it, and create additional market pressure for all stakeholders in the health

ecosystem to embrace best-in-class MFA solutions. The disclosure should indicate the method of access to the information and if MFA was implemented.

3. Acknowledge that best practices in authentication often go beyond use of traditional MFA (looking at factors of something people have/know/are). We believe the industry should continue to pursue options for secure, password-less authentication standards. Therefore, complementing those products with tools such as behavioral biometrics and risk-based analytics to deliver “Continuous Authentication” will be helpful. While NIST has not yet updated SP 800-63B to reflect the emergence of these tools, they are commonly used in the marketplace to provide additional authentication security, and many purchasers of health IT products will be interested in whether these products support this technology. Allowing vendors to disclose their use of Continuous Authentication technology will encourage innovation and provide additional transparency for the authentication capabilities included in certified health IT products.

#### **Section VII.B.4 Application Programming Interfaces (APIs)**

§170.315(g)(10) Standardized API for patient and population services:

The proposed technical outcomes and conditions are insufficient to assure the security of the information system ecosystem or the patient data to be transported through the API. **We recommend additional standards to advance the confidentiality, integrity and availability (CIA)<sup>1</sup> of electronic health information (EHI) that will be handled by an API and to reduce the risk of threats and vulnerabilities that could be introduced into an information system to which the APIs could connect.** One example would be to require suppliers to demonstrate that threats and vulnerabilities found through a risk-based assessment have been addressed to minimize the risk to the CIA of the EHI.

§170.404 Application programming interfaces (Condition and Maintenance of Certification):

The proposed Condition and Maintenance of Certification requirements are insufficient to assure the security of the information system ecosystem or the patient data to be transported through the API. **An API technology supplier should have service and support obligations to conduct surveillance and mitigate threats and vulnerabilities to the confidentiality, integrity and availability of EHI that will be handled by an API, as well as to reduce the risk of threats and vulnerabilities that could be introduced into an information system to which the API could connect.**

#### **Section VII.B.5 Real World Testing**

We believe requiring providers and health information networks (HINs) to provide access to their information systems prior to the implementation of the requirements for real world testing creates an unreasonable threat to patient safety and information security of the health care ecosystem. The preamble comment to Section VII.B.5 recognizes that the adoption of a final rule will come too late to permit health IT developers to submit a real world testing plan and/or

---

<sup>1</sup> The definitions of *Confidentiality, Integrity and Availability* at 45 CFR §164.302

perform and report testing results of its API technology, including any detrimental impact to patient safety or information security of the healthcare ecosystem. **We recommend a delay of the enforcement date of the standards for information blocking for 12 to 18 months after the effective date of the final rule to allow sufficient time for suppliers to meet the standards for Real World Testing.**

## **Section VIII Information Blocking**

### §171.00 Statutory Basis and Purpose

Several provisions of the proposed rule would have the effect of modifying or substantially altering the standards and implementation specifications of the HIPAA Privacy Rule (45 CFR §§ Parts 160 and 164 subpart E). In adopting section 3022 of the Public Health Service Act, (42 U.S.C. 300jj-52) the Congress did not amend or exhibit an intention to modify or curtail the provisions of the HIPAA Privacy Rule standards. **We recommend that HHS substantially revise the provisions of the Information Blocking proposal to remove those provisions that would have the effect of altering or modifying the standards or implementation specifications of the Privacy Rule.**

### §171.102 Definitions

*Health care provider:* We recommend that the definition be revised to apply only to those individuals or organizations subject to the HIPAA Administrative Simplification Standards (e.g. covered entities and business associates). The proposed definition would encompass health care providers that have no current federal or state requirements for the use and disclosure of EHI (e.g. educational institutions, non-HIPAA covered health care providers). These providers would be subjected to a significant burden to procure and implement needed technology to exchange or transmit EHI, and to develop and implement the policies and procedures that would be required to comply with the Information Blocking regulations.

### **Comment regarding practices that may implicate the information blocking provision**

The circumstances described present a likelihood that a practice will interfere with access, exchange, or use of EHI within the meaning of the information blocking provision. The preamble's discussion of the Privacy Rule's Right of Access (45 CFR § 164.524(a)) is incomplete and out of alignment with HIPAA. While the patient or their personal representative has the right to access PHI, the covered entity (or their business associate) is required to implement policies and procedures for requests to access and to ensure that the covered entity acts on the request no later than 30 days after receipt (see 45 CFR §164.524(b)(2)). Requiring a Provider or health information network (HIN) to immediately provide access to the EHI under the Information Blocking provisions inappropriately modifies and undercuts these provisions of the Privacy Rule and is outside the scope of ONC's authority under the 21<sup>st</sup> Century Cures Act.

In addition, the implementation of the Information Blocking provisions will impose expensive and time-consuming burdens in order to modify current policies and procedures required under the Privacy Rule. Additional burden will result from modification of the Notice of Privacy Practices (45 CFR §164.520) required under the Privacy Rule due to the changes in the organization's

policies and procedures required to comply with the Information Blocking provisions. The Proposed Rule does not account for or estimate the burden that providers or other actors will incur to comply with the Information Blocking provisions.

The Information Blocking proposal's definition of EHI is broader than the Privacy Rule's definition of Protected Health Information (PHI) (45 CFR §160.103) and requirements for information blocking include vague, subjective, and undefined terms (e.g., timely, burdensome, network). This vagueness will create uncertainty as to whether information blocking could be validated by HHS and therefore lessen the benefit of this important 21<sup>st</sup> Cures provision (e.g., what is EHI?). Health care providers do not currently account for individually identifiable health information beyond PHI and may not incorporate such data into their EHRs. These providers and other actors will require significant time to identify what EHI is maintained electronically and to consolidate the data into a system that would allow access to the patient or their representative. The United States Core Data for Interoperability (USCDI), however, provides objective structure with standards that moves us closer to a computable medical record. **ONC should direct its focus on alignment with information blocking and the certified capabilities of health IT vendors (i.e., USCDI and APIs).** A logical, objective approach to promoting interoperability is necessary to reduce confusion. In other words, information blocking should be evaluated through the lens of access, use, and exchange of the USCDI.


#### **Privacy of information shared through apps**

ONC has not indicated that it will create a policy to help ensure patient privacy protections through the use of APIs. In other words, it is promoting API usage, but not requiring that the API technology include privacy and security controls. If patients access their and their family's health data—some of which is likely sensitive—through a smartphone, patients must have a clear understanding of the potential uses of that data by app developers. To increase transparency ONC could require an EHR vendor's API to check for the following "yes/no" adoption and implementation attestations from an app as a part of the EHR vendor's certification requirements:

- *Industry-recognized development guidance* (e.g., [Xcertia's Privacy Guidelines](#));
- *Transparency statements and best practices* (e.g., [Mobile Health App Developers: Federal Trade Commission Best Practices](#) and [CARIN Alliance Code of Conduct](#)); and
- *A model notice to patients* (e.g., [ONC's Model Privacy Notice](#)).

Thank you for the opportunity to comment. We would be pleased to answer any questions about this submission.

Sincerely,

  
Greg Garcia, Executive Director  
HSCC Cybersecurity Working Group