AMA
AMERICAN MEDICAL
ASSOCIATION

JAMES L. MADARA, MD
EXECUTIVE VICE PRESIDENT, CEO

ama-assn.org
t (312) 464-5000

May 31, 2019

Don Rucker, MD
National Coordinator for Health Information
Technology
Office of the National Coordinator for
Health Information Technology
U.S. Department of Health and Human Services
330 C Street, SW
Washington, DC 20201

Re: 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program proposed rule

Dear Dr. Rucker:

On behalf of the physician and medical student members of the American Medical Association (AMA), I am pleased to offer our comments to the Office of the National Coordinator for Health Information Technology (ONC) on the Interoperability, Information Blocking, and the ONC Health Information Technology (Health IT) Certification Program proposed rule.

The following outlines our principal recommendations on ONC's proposed rule:

- The AMA supports ONC's proposal to require all certified health IT systems to comply with the U.S. Core Data for Interoperability version 1 (USCDI v1). The AMA urges ONC to prioritize its effort to establish and follow a predictable, transparent, and collaborative process to expand the USCDI, including providing stakeholders with the opportunity to comment on the USCDI's expansion.

- The AMA supports ONC's proposal for certified health IT developers to adopt and implement new requirements around application programing interface (API) design, function, and use. This will enhance interoperability and reduce implementation complexity and cost. We support requiring the adoption of Fast Healthcare Interoperable Resources (FHIR) Release 4 and compliance with HL7 U.S. Core FHIR Implementation Guides.

- The AMA appreciates ONC's efforts to address excessive fees charged by electronic health record (EHR) vendors to connect their products with other health IT systems, health information exchanges, and third-party applications. ONC's proposal fee policy attempts to address most scenarios, but the resulting framework is complex and has limited usefulness for physicians. We suggest a more practical approach that includes a tiered fee structure for APIs. For instance, ONC could establish categories where the technology requirements designate the fees.

- Data segmentation is critical for health information exchange, regardless of where the data resides, how it is used, or with whom it is exchanged. Patient consent and privacy, data provenance, governance, and state and federal law compliance must be inherent in technology development. The AMA supports Consent2Share (C2S) as a Base EHR requirement and encourages ONC to increase C2S adoption.

- The AMA supports the need to limit information blocking. Practical regulation is required to establish guiderails for electronic health information (EHI) and exceptions for information blocking practices. However, ONC's EHI and information blocking proposals are too vague. A logical, objective approach is necessary to reduce confusion. ONC should align its information blocking requirements with the certified capabilities of health IT vendors—i.e., the USCDI and APIs. Information blocking should be evaluated through the lens of access, use, and exchange of the USCDI.

- The AMA supports the use of APIs and consumer-facing applications (apps). ONC's proposal includes numerous policies that seek to promote app developers' access and use of EHI. However, the AMA has serious concerns with apps being provided equal protections and benefits with those of patients. Concerningly, apps frequently do not provide patients with clear terms of how that data will be used—licensing patients' data for marketing purposes, leasing or lending aggregated personal information to third parties, or outright selling it. These practices jeopardize patient privacy, commoditize an individual's most sensitive information, and threaten patient willingness to utilize technology to manage their health. Patients should be the primary authority in designating rights to access, exchange, and use of their data. ONC should require that all certified APIs include mechanisms to strengthen patients' control over their data.

- The AMA recognizes the potential benefits of bulk data access for public and population health and quality improvement. However, we have concerns with the potential pitfalls of entities having unprecedented access to patient information. Important parameters must still be established to maintain patient privacy, data security and usability, and adherence to federal and state law. We urge ONC to take a methodical approach in its promulgation of information blocking and EHI regulation.

- The AMA supports maintaining the Health Insurance Portability and Accountability Act's (HIPAA) minimum necessary standard. However, the proposed rule conflates payers' needs with clinicians' needs to access, exchange, or use health information. Physicians must be permitted to retain their professional judgment to protect their patients' rights or privacy, including their designation for what constitutes minimum necessary.

- AMA research has shown that cyberattacks are inevitable and increasing, and numerous agencies across the federal government recognize cybersecurity as a patient safety issue. ONC's policy allowing an actor (e.g., a consumer-facing app developer) the ability to *read, write,* and *modify* a patient's entire medical record invites cyber-attacks. ONC should do more to ensure EHR vendors develop and test to industry protective measures, prescribed standards, and security protocols.

- The AMA has concern with ONC's interpretation of Health Information Networks (HINs) and other terms. ONC's definitions are inconsistent. This creates separate interpretations, adds subjectivity, and introduces unnecessary vagueness and inconsistency. We strongly recommend that the definition of HIN be narrowed to include only entities that are an actual network (or formalized component of an actual network) and have an actual operational role and responsibility for the network.

- The AMA supports many of the proposals for certified EHR technology (CEHRT). However, ONC's physician adoption timeline is incredibly ambitious and usurps CMS' authority to determine EHR adoption. To prevent significant confusion for physicians about program requirements, we strongly recommend ONC refrain from adjusting the 2015 Edition Base EHR definition and recommend naming a new Edition.

The AMA proudly supported several health IT provisions in the 21st Century Cures Act (Cures). The iterative introduction of information technology in health care has been around for decades. The passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act quickened the pace of EHR adoption and use. Early after its passage, the AMA recognized the potential to improve patient care and reduce costs through the digitization of health information. However, the AMA also had the prescience to identify unintended consequences of hastily deploying health IT without a well-thought-out plan and priorities. Lacking fundamental elements to facilitate safe, effective, and interoperable EHRs, patients and physicians would be negatively impacted. Health IT would stray from being a clinical benefit to a burden. Our concerns have largely been proven right.

The passage of Cures provides an opportunity to correct the course of health IT. Congress wisely included provisions addressing physician burden, EHR usability and vendor practices, interoperability, information blocking, and patient information empowerment. ONC has taken up this charge and proposed a sweeping set of changes to health IT certification as well as a thorough interpretation of congressional intent. **Several of the proposed changes, especially around health IT vendor practices and EHR performance, are welcome and respond to concerns raised by the AMA and clinical community.**

The AMA has also identified proposals that could prove problematic and run counter to the goals Congress set out to achieve in Cures. **ONC's broad interpretation of legislative language, compressed development and adoption timelines, complex regulatory requirements, and a misplaced emphasis on data quantity will dramatically impact patient privacy and safety, data security, and further exacerbate physician burden and concerns with health IT.** Without addressing these issues, the U.S. Department of Health and Human Services (HHS) may fail at meeting the goals set out by Congress in Cures.

Opportunities to Improve Health IT

The ability to access the right medical information at the right time for the right individual are three needs most often cited as the potential of health IT. Achieving this "triple need" requires an orchestration of technical capability (validated through testing), trust between parties (established through transparent practices), and consistency in data structure and meaning (agreed upon common data models). Together, these three pillars support the access, exchange, and use of electronic health information. **Cures' provisions reinforce these goals**:

- Interoperable technology must "enable the secure exchange of electronic health information with, and use of electronic health information from, other health information technology without special effort on the part of the user."[1] It takes a significant amount of effort (both in time and resources) to use unstructured electronic health information. Structure helps retain information's original meaning. Moreover, structure helps prevent quality degradation of the patient's record.

- Cures states that certified health IT developers are required to successfully test the "real world use of the technology for interoperability."[2]

- A national framework must establish a "common set of rules for trusted exchange."[3]

- HHS must also "promote patient access to health information in a manner that would ensure that such information is available in a form convenient for the patient, in a reasonable manner, without burdening the health care provider involved."[4]

Congress intentionally promotes a consistent theme of data *usability* across Title IV of Cures. Each provision creates a narrative, and when read together, tell a cohesive story. Forgoing data use for quantity, or sacrificing data value for volume, would miss the clear message in Cures—data needs to be accessible, but also understandable and actionable.

The AMA supports patients and physicians having electronic access and use to medical records. The digitization of records through EHRs should have reduced the friction of collecting, organizing, and sharing of data. Unfortunately, digital records are only part of the equation. For instance, ONC's previous certification efforts addressed data structure but lacked focus on implementing technology consistently across EHRs. Efforts by others to establish governance models for trusted exchange practices lacked oversight to ensure a uniform understanding of shared medical information. Coordination has been lacking; no one party is at fault.

ONC's proposed rule takes important steps to address multiple issues. It includes updates to standards, certification, and vendor requirements that will help improve interoperability, EHR performance, and data use. **Consistent with AMA's recommendations, ONC is promoting greater access to structured data elements, requiring the widespread use of APIs, and limiting excessive fees and contractual limitations that prevent interoperability.** The AMA supports these concepts along with several of ONC's proposals to advance them. We appreciate ONC providing a comment template for its proposed rule; additional feedback can be found in the attached appendices.

U.S. Core Data for Interoperability

The AMA supports ONC's proposal to require all certified health IT systems to comply with the USCDI v1. ONC identifies the USCDI as a standardized set of health data classes and constituent data elements

[1] Cures Sec. 4003.
[2] Cures Sec. 4002.
[3] Id.
[4] Cures Sec. 4006.

for nationwide, interoperable health information exchange.[5] Currently, the data that is "exposed" by an EHR (e.g., the common clinical data set, or CCDS) is often a subset of what most would consider a complete medical record. Health IT vendors can provide data beyond the required minimum but have historically not gone beyond certification requirements. **Ultimately, all health IT should provide access and use of a patient's entire longitudinal medical record in a computable format. The need for better usability, however, should not be trumped by the demand for more data.** "Perfect" may be all electronic health information, but "good" is what can practically be accessed, used, or exchanged; we should not let perfect be the enemy of good. Information that is necessary to coordinate care should be structured for optimal usability. Not all data needs to be standardized, but it should be computable. **The USCDI provides objective structure with standards that moves us closer to a computable medical record.** We agree with ONC that "the USCDI standard aims to achieve the goals set forth in the Cures Act by specifying a common set of data classes for interoperable exchange," but much more needs to be done.

The AMA urges ONC to prioritize its effort to establish and follow a predictable, transparent, and collaborative process to expand the USCDI, including providing stakeholders with the opportunity to comment on the USCDI's expansion. The accelerated addition of data classes and elements—along with additional context around these data (i.e., metadata)—is vital to meeting the goals of Cures. It is also logical to include pricing, cost, and administrative transaction standards in the USCDI version expansion. This will support the Administration's goal to bolster a health care market economy, facilitate price transparency, and vastly expand the number of ways in which a beneficiary can access and utilize such information. Additionally, coding and terminologies that support a patient's use of his or her health information will become increasingly vital. Descriptors that support the translation of medical jargon into consumer-friendly information should be leveraged. **Immediately following the publication of its final rule, ONC should establish a formal USCDI submission, review, and validation process to ensure clinician perspectives are considered.** As ONC considers the structure and processes necessary to expand the USCDI, the AMA recommends ONC adopt the Health Information Technology Advisory Committee (HITAC) USCDI Task Force's recommendations dated April 18, 2018. This is a critical need to build consensus across the health care system. The AMA is uniquely qualified to support this effort.

The AMA has established an Integrated Health Model Initiative (IHMI) that leverages collaborative communities, a physician-led validation and review process, and advanced data modeling to support improvement in data use and exchange. IHMI is recognized by ONC's Interoperability Proving Ground and by the Health Information Technology Advisory Committee's Interoperability Standards Priorities Task Force. IHMI works with over 30 health care stakeholders, including major technology developers, informaticists, terminologists, consumer groups, professional associations, clinicians, and standards development organizations. **The AMA offers our IHMI to support cross-stakeholder agreement related to data standardization/modeling, medical knowledge representation, and efforts around data portability/liquidity.**

[5] U.S. Core Data for Interoperability, 2019 version 1, available at: https://www.healthit.gov/isa/sites/isa/files/inline-files/USCDIv12019revised.pdf.

APIs for Health Care

The AMA supports ONC's proposal for certified health IT developers to adopt and implement new requirements around API design, function, and use. This will enhance interoperability and reduce implementation complexity and cost. Cures solidified the importance of APIs by requiring that health IT:

> …has published application programming interfaces and allows health information from such technology to be accessed, exchanged, and used without special effort through the use of application programming interfaces or successor technology or standards, as provided for under applicable law, including providing access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws.[6]

Health IT must also support "patient access to their electronic health information, including in a single longitudinal format that is easy to understand, secure, and may be updated automatically."[7] Again, each Cures provision paints a narrative. Consistently structured data elements, accessed through secure APIs, are key to data usability. Standards-based APIs help people know the context of data, where it fits in the workflow, and what "language" was used. Individuals receiving that data can then interpret the intended meaning consistently and safely, providing valuable *information*—not just "noise"—to the user.

The AMA recognizes that common implementation specifications and implementation guides focus developers' efforts. **We support requiring the adoption of FHIR Release 4.** This is the first normative version, supporting enhanced capabilities, and offering backwards compatibility. Profiles and implementation guides further constrain FHIR for use cases. That said, it is still possible to create data that is not computably equivalent. Wherever possible, ambiguity should be removed so data are more computationally equivalent and comparable. **The AMA supports ONC's proposal of USCDI and the API Resource Collection in Health (ARCH) to achieve this.**

ONC should require compliance with HL7 U.S. Core FHIR Implementation Guides derived from the Argonaut implementation guides, rather than the Argonaut implementation guides themselves. Where HL7 Implementation Guides are not available for the corresponding and required Argonaut functionality, ONC should facilitate their inclusion as HL7 standards. Argonaut is a closed membership group with no opportunity for many stakeholders, such medical professional organizations, to provide input—whereas HL7 is an open-member, ANSI-accredited standards development organization, which enables such stakeholder input.

The AMA appreciates ONC's efforts to address excessive fees charged by EHR vendors to connect their products with other health IT systems, health information exchanges, and third-party applications. We recognize that API permitted fees and restrictions are a multi-pronged issue. Developing policy to accommodate every interaction between an API Technology Supplier, API Data Provider, and API User is untenable. While ONC has attempted to address most scenarios, the resulting proposed fee policy is complex and has limited usefulness for physicians. Our members are already expressing concerns over the increased costs they will encounter to hire consultants or seek legal support just to parse out the rights and responsibilities of each API actor. We are concerned the proposed fee structure will ultimately

[6] Cures Sec. 4002.
[7] Cures Sec. 4006.

designate physicians as the default revenue stream for EHR vendors and app developers.

The AMA believes a more practical approach would be to establish a tiered fee structure for APIs. For instance, ONC could establish categories where the technology requirements designate the fees.

- A "no fee" category would limit API Technology Suppliers from charging API Data Providers or API Users any fees for exchanging data in compliance with federal requirements (e.g., costs associated with health information exchange, patient access, reporting quality measures, and data segmentation for privacy). Since all API Technology Suppliers will be certified by ONC, any API Technology Supplier-to-API Technology Supplier connections would also be in the "no fee" category.
- An "at cost" category would allow API Technology Suppliers to charge API Data Providers or API Users the cost of interfacing APIs with a non-API Technology Supplier's commercial technology (e.g., commercial lab systems, commercial picture archiving and communication systems (PACS), commercial data analytics services).
- A "cost plus reasonable profit" category would allow API Technology Suppliers to charge API Data Providers or API Users a reasonable profit when conducting legitimate custom API development or creating custom apps (e.g., creating proprietary mappings for technology unique to a health system or establishing connections with non-commercially available technology).

For the "at cost" and "cost plus reasonable profit" categories, API Technology Suppliers should be restricted from implementing health IT in non-standard ways that unnecessarily increase the costs, complexity, and other burden of accessing, exchanging, or using EHI. We do not expect all scenarios will be addressed by this approach; however, we believe a clearer and more approachable fee structure will better empower physicians to be informed consumers of technology. We believe this also establishes fair and equitable fee structure for all parties involved.

Scope of Information Blocking

ONC's interpretation of Cures' terms "information blocking" and "EHI" places major expectations on the actors involved. The AMA urges caution to consider downstream consequences of being too broad or expansive. We are very concerned that EHI and information blocking proposals are too vague, using many undefined terms (e.g., timely, burdensome, network, etc.). This vagueness creates uncertainty around whether information blocking can be objectively evaluated and validated by HHS, potentially weakening this important Cures provision. A logical, objective approach to promoting interoperability is necessary to reduce confusion. The USCDI provides such structure, using standards that move us closer to a computable medical record. As such, **ONC should align its information blocking requirements with the certified capabilities of health IT vendors—i.e., the USCDI and APIs. In other words, information blocking should be evaluated through the lens of access, use, and exchange of the USCDI.**

Bulk Data Access

FHIR Release 4 sets the stage for greater data analytics. Medicine can benefit from sophisticated analyses of populations of patients, larger data sets, and the combination of clinical and social risk factors. Work to enable FHIR bulk data extract (i.e., the electronic collection of data composed of information from multiple records) is ongoing but running on a different timeline than Release 4. **Accessing patients' information at this scale still requires important parameters to be established to maintain patient privacy, data security and usability, and adherence to federal and state law.** The AMA anticipates that FHIR-based APIs will eventually provide enhanced access, use, and exchange of EHI. The AMA is tracking these opportunities closely and participating in community efforts like HL7's Da Vinci Project.

The AMA recognizes the potential benefits of bulk data access for public and population health and quality improvement. Reducing the difficulties inherent in accessing medical information at the individual or population health level is an important goal; however, we have concerns with the potential pitfalls of entities having unprecedented access to patient information. **We urge ONC to take a methodical approach in its promulgation of information blocking and EHI regulation. ONC should ensure the physician and patient communities are clear, well-informed and agree with efforts to advance data access at the levels proposed.**

The AMA is not alone in these concerns. The CARIN Alliance, a multi-sector group of stakeholders representing numerous hospitals, thousands of physicians, and millions of consumers, individuals, and caregivers recently provided to the National Coordinator comments the exchange of EHI. CARIN stated:

> End Users should have access only to the information they need for a given purpose, consistent with the HIPAA Privacy Rule's minimum necessary standard. We agree that reducing the friction of accessing medical information at the individual or population health level is an important goal; however, we have concerns with the potential pitfalls of stakeholders having unprecedented access to information across the health care system. Current data request processes, while limiting, are narrowly scoped for specific use cases and involve some level of "gating" that helps prevent abuse and helps enforce compliance with minimum necessary standard on both ends of the transaction (collection (query) and disclosure). Automating and increasing the volume of data access, without some mechanisms in place to help enforce minimum necessary at both ends, may invite misuse. We strongly recommend that ONC consider all ramifications of bulk data access, including an individual's privacy and security of their information, and situations that inadvertently result in "select all & copy." Clearly, increasing ease of access to data is an imperative; however, ONC must also consider the need to hold entities accountable, including assuring that covered entity End Users can comply with their minimum necessary obligations in both launching and responding to queries.[8]

Information Blocking Exceptions and Sub-Exceptions

The AMA appreciates ONC's recognition through proposed exceptions to information blocking that physicians may have valid, reasonable cause to restrict exchange of information. We highlight, however, that the proposed requirements are overly complex, riddled with subjective terminology, and demand policy and procedure documentation above and beyond practicality. The proposed burden of proof is unreasonable and the need to demonstrate that a policy is sufficiently tailored is likely to create a costly

[8] CARIN Alliance letter to Dr. Don Rucker, *21st Century Cures Act Trusted Exchange Framework and USCDI Public Comments*, available at: https://www.carinalliance.com/wp-content/uploads/2019/04/CARIN_TEFCA_comments_FINAL_02202018.pdf.

compliance burden. It is not entirely clear how ONC intends to educate physicians on the multitude of permutations that would and would not constitute information blocking. Exceptions need to be more commonsense. As such, **for each information blocking exception ONC should clarify that a physician's professional judgment will never be considered information blocking.** This, coupled with aligning information blocking and EHI requirements with USCDI and certified APIs, will reduce the overall complexity of ONC's proposal.

Patient Privacy and Data Security

Privacy is a critical consideration of health information exchange, regardless of where the data resides, how it is used, or with whom it is exchanged. Congress repeatedly cites the importance of privacy and security throughout Cures—including the concepts in almost every major health IT provision. Congress saw fit to include privacy and security when directing HHS to develop a general health IT strategy; removing "gag clauses" on communicating health IT issues; requiring public reporting on EHR performance; describing a national trusted exchange framework; establishing priority target areas and standards for the Health IT Advisory Committee (HITAC); contemplating what would not be considered information blocking; and studying the need to correctly match patients with their records. Multiple provisions create a narrative, and when read together, tell a cohesive story. **Clearly, Congress' intent was to ensure any actions to advance the access, exchange, or use of health information must also <u>strengthen</u> the privacy and security of that data.**

AMA Approach to Privacy and Security

The first step of any ultimately successful privacy framework, legislative or regulatory, places the patient first. Each entity seeking access to patients' most confidential medical information must pass the stringent test of showing why its professed need should override individuals' most basic right in keeping their own information private—something that technology should help physicians accomplish in a minimally burdensome way. Moreover, citizens deserve a full and open discussion of exactly who wants their private medical information and for what purpose. Only then may the true balancing of interests take place. These are the ground rules of AMA policy and they should be the ground rules for patient privacy.

The AMA's approach to privacy is governed by our Code of Medical Ethics and long-standing policies adopted by our policymaking body, the House of Delegates, which support strong protections for patient privacy and, in general, require physicians to keep patient medical records strictly confidential. **AMA policy and ethical opinions on patient privacy and confidentiality provide that a patient's privacy should be honored unless waived by the patient in a meaningful way, de-identified, or in rare instances when strong countervailing interests in public health or safety justify invasions of patient privacy or breaches of confidentiality.**

These policies and ethical opinions are designed not only to protect patient privacy, but also to preserve the patient-physician relationship. This is particularly important in scenarios involving sensitive health information. For example, striking the correct balance is critical in encouraging individuals with mental illness and/or substance use disorders (SUD) to seek treatment. Consumers are also increasingly concerned with privacy in today's environment (e.g., the Facebook–Cambridge Analytica data scandal). **In fact, many industries, states, and countries are moving towards increasing privacy rights and protections, not expanding ways in which information can be shared without an individual's full knowledge and clear consent.**

Health care information is one of the most personal types of information an individual can possess and generate—regardless of whether it is legally defined as "sensitive"—and policymakers must be very cautious in discussions of how to encourage greater access. **We must always ask whether relaxing privacy controls will encourage patients to seek care or potentially deter them.** Privacy risks include re-identification of patients through de-identified (or partially de-identified) data, misunderstanding or disregard of the scope of a patient's consent, patient perception of loss of their privacy leading to a change in their behavior, embarrassment or stigma resulting from an unwanted disclosure of information or from fear of a potential unwanted disclosure, perceived and real risks of discrimination including employment and access to or costs of insurance, and law enforcement accessing data repositories beyond their intended scope.

Physicians take the Hippocratic Oath to "do no harm" and swear that "whatever I see or hear in the lives of my patients, whether in connection with my professional practice or not, which ought not to be spoken of outside, I will keep secret, as considering all such things to be private."[9] **Physicians want to share patent's information where appropriate. However, maintaining trust between patients and physicians is fundamental to medicine.**

Presumption of Guilt Around Information Blocking

As discussed above, physicians may have a valid, reasonable reason to restrict the exchange of information. **Yet ONC's interpretation of Cures creates an assumption that any physician who withholds data is guilty of information blocking.** To counter this assumption and to justify withholding information for any reason, physicians must divert time and resources away from patient care to dissecting incredibly complex exceptions that are riddled with subjective terminology. Once a physician does so (potentially by hiring attorneys or consultants at great expense to the practice), he or she must create new policies and procedures, train staff, and adjust workflows. Furthermore, physicians may need to document the justification for applying those exceptions for every single request of information. The inherent presumption of guilt, complex sub-exceptions, and substantial added burdens of ONC's proposal exceed the scope of Cures' intent. ONC should create policies that identify bad actors without placing considerable burden on the rest of the health care system. Otherwise physicians will be tasked, time and time again, with the chore of documenting decisions that should be left to the physician's best judgement. Or, alternatively, they will just share whatever information they are asked for, regardless of whether the requestor has valid reasons for doing so, and the physician risks penalties for that, too. In either scenario, physicians and patients lose.

By way of example, we highlight ONC's proposed minimum necessary exception and its effect on patient privacy. Prioritizing data quantity over usability presents significant privacy concerns. For example, a directive to exchange all EHI with any requestor for nearly any purpose may force physicians to compromise the "minimum necessary" standard in HIPAA. **The AMA supports maintaining HIPAA's minimum necessary standard, which generally requires physicians to share the minimum amount of information necessary to accomplish the intended purpose of the disclosure.**[10] For instance, we do not support requirements to disclose an entire designated record set to another covered entity. We also do

[9] Hippocratic Oath, U.S. National Library of Medicine, available at: https://www.nlm.nih.gov/hmd/greek/greek_oath.html.

[10] 45 CFR §164.502(b).

not support a requirement to disclose psychotherapy notes—we note that even patients do not have access rights to their psychotherapy notes. Minimum necessary controls are particularly important given the Administration's clear intent to promote the exchange of information above all else and the emerging capability of technology to extract bulk patient data out of an EHR.

Confusion about HIPAA's minimum necessary standard versus ONC's EHI-based information blocking requirements will lead to oversharing of patient data. Some clinicians may find it easier (and less worrisome from an enforcement perspective) to simply disclose everything they have. Additionally, the Meaningful Use Program demonstrated that when requirements to exchange data exist, but lack minimum necessary standards, health care organizations will send everything to ensure they comply with the requirement to exchange.[11,12,13] The receiving physician is then saddled with the enormous burden of reviewing all the information to glean what is clinically relevant. Furthermore, while we appreciate ONC's inclusion of a minimum necessary sub-exception, the efforts required to assert the sub-exception are excessive. Attempting to determine how much information to divulge so as not to violate HIPAA and face OCR enforcement or ONC's information blocking rules (evoking OIG enforcement) amounts to significant cognitive burden. Those who do make such determinations are required to create new policy and procedures[14] and navigate multiple exceptions or sub-exceptions. Both scenarios are a result of increased regulatory complexity that contradicts Congress' intent to reduce physician burden.

Exploiting the link between minimum necessary and information blocking requirements may also lead to "bullying." For example, physicians already have established processes to determine what constitutes the minimally necessary amount of information to process claims. This balances adjudication needs with clinical judgment and patient privacy. As proposed, EHI and information blocking requirements may empower payers to demand more information than is needed. Patients trust physicians to safeguard access to their most personal information, only sharing it for appropriate purposes and with their consent. We highlight that, while ONC repeatedly promotes payers' access to data, Congress refrained from mentioning payers in Cures' information blocking provision. **ONC seems to conflate the interests of payers with clinicians' need to access, exchange, or use health information.** Further, payers are not subject to information blocking requirements and are therefore emboldened to use (and withhold) information as they see fit. Unfortunately, under ONC's proposal, a physician who denies a payer's request for EHI—regardless of whether the request is fully warranted—may implicate the physician in information blocking.

[11] Dr. David Barbe, President-elect American Medical Association, *EHR Innovation and Problem-Solving: Physician Perspective*, 2016, available at: https://www.healthit.gov/sites/default/files/David_Barbe-Innovation_&_Problem-Solving.pdf.

[12] Reisman, Miriam, *EHRs: The Challenge of Making Electronic Data Usable and Interoperable*, P & T : a peer-reviewed journal for formulary management vol. 42,9 (2017): 572-575, available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5565131/.

[13] EHR Intelligence, *GAO: Lack of data standards foils EHR interoperability, HIE*, 2014, available at: https://ehrintelligence.com/news/gao-lack-of-data-standards-foils-ehr-interoperability-hie.

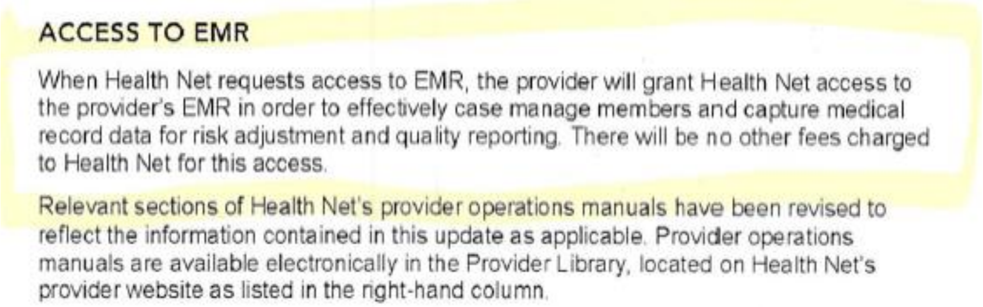
[14] ONC proposes that for an actor to qualify for an information blocking sub-exception, the actor's privacy policies and procedures would need to identify criteria for making a "minimum necessary" determination for both routine and non-routine disclosures and requests, including identifying the circumstances under which disclosing the entire medical record is reasonably necessary. HIPAA only requires policy determinations be established for non-routine disclosures.

To address concerns not only with minimum necessary standards, but the misguided approach to presumption of guilt around information blocking, **ONC should clarify that a physician exercising his or her best judgement when providing information to a requestor will not be considered an information blocker. ONC should also remove onerous requirements for physicians to document their decision-making associated with qualifying for information blocking exceptions or sub-exceptions.**

Concerns with Overreach

The AMA has continuously maintained that an expressed "need" for information—including for care coordination purposes—does not confer a right to such information, particularly when it conflicts with a patient's wishes. Some parties may reject this principle as too deferential to patients' rights at the expense of administrative feasibility. However, the AMA believes that this approach properly balances the interests at stake. **We strongly urge ONC to clarify that a physician's professional judgment to protect their patients' rights or privacy will never be considered information blocking. We again stress that policy and procedure requirements within information blocking exceptions should forgo adding confusion, complexity, or burden to physicians' medical practices.**

We anticipate that some commenters will suggest that payers be able to leverage information blocking and EHI requirements to relieve burden on the patient and physician—in fact, some payers are already doing it, either as an elective offering[15] or through a contractual requirement (see screenshots pasted in below).



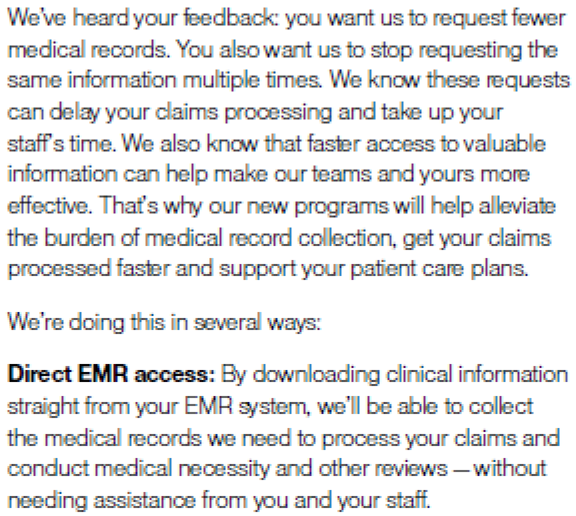
ACCESS TO EMR

When Health Net requests access to EMR, the provider will grant Health Net access to the provider's EMR in order to effectively case manage members and capture medical record data for risk adjustment and quality reporting. There will be no other fees charged to Health Net for this access.

Relevant sections of Health Net's provider operations manuals have been revised to reflect the information contained in this update as applicable. Provider operations manuals are available electronically in the Provider Library, located on Health Net's provider website as listed in the right-hand column.

Excerpt from HealthNet Provider Update (March 21, 2019)

[15] UnitedHealthcare Enterprise Medical Records Program: An Easier Way to Share Medical Records, https://www.uhcprovider.com/en/resource-library/uhc-enterprise-medical-records.html.



We've heard your feedback: you want us to request fewer medical records. You also want us to stop requesting the same information multiple times. We know these requests can delay your claims processing and take up your staff's time. We also know that faster access to valuable information can help make our teams and yours more effective. That's why our new programs will help alleviate the burden of medical record collection, get your claims processed faster and support your patient care plans.

We're doing this in several ways:

Direct EMR access: By downloading clinical information straight from your EMR system, we'll be able to collect the medical records we need to process your claims and conduct medical necessity and other reviews — without needing assistance from you and your staff.

Excerpt from UnitedHealthcare Network Bulletin[16] *(October 2018)*

Physician practices may not understand that this level of access could lead to selective, discriminatory reimbursement models and intrusion on physician medical decision-making power (e.g., lower reimbursement rates for certain types of care that a physician deems necessary or in the best interest of the patient). There are already examples of payers making coverage decisions based on patient information their physicians were not aware of.[17] Further, physician practices could be priced out of markets because a payer determines that they are a "second or third-tier" option based on access to EHR data. **We strongly oppose any type of automatic, unfettered payer access to a physician's EHR, including through the interpretation of EHI and information blocking regulations.** Such access requires privacy and security guardrails that have not been adequately discussed in this rule. A payer must not be permitted to use regulation to force physicians to provide access to their EHRs. **We again recommend ONC align information blocking requirements around the USCDI and certified APIs.** This will help reduce the unintended consequences of abuse or overreach into patients' medical records. Clearly, increasing ease of access to data is important; however, ONC must not inadvertently incentivize bad behavior.

Data Privacy Controls

FHIR supports data controls like segmentation; however, we are concerned those controls are an afterthought in FHIR-based API design and will become "bolt-on" functions—drastically increasing their costs and limiting their usefulness. The AMA has been told that FHIR developer efforts are first focused on "just making the technology work" and that "patient data protections and privacy controls are outside their scope." The downstream consequences of this approach will negatively impact physicians and

[16] UnitedHealthcare "pitches" this as a voluntary convenience for physicians, however, does not include language about how it will ensure limited access records. ONC's information blocking proposals will further cloud how much access should be allowed.

[17] National Public Radio, *You Snooze, You Lose: How Insurers Dodge The Costs Of Popular Sleep Apnea Devices*, 2018, available at: https://www.npr.org/sections/health-shots/2018/11/21/669751038/you-snooze-you-lose-how-insurers-dodge-the-costs-of-popular-sleep-apnea-devices.

patients. Mechanisms to monitor and control data access, patient consent and privacy, and ensure data provenance, governance, and enforce state and federal law must be inherent in FHIR development.

Existing standards such as Consent2Share (C2S) and Data Segmentation for Privacy (DS4P) are not being utilized due to cost, maturity, or lack of adoption. We appreciate that ONC is proposing C2S and DS4P as optional certification criteria for health IT and that the DS4P proposal requires segmentation at the element level (as opposed to the document level). We understand that DS4P is viewed as a major development challenge for EHR vendors. In discussing privacy with the Substance Abuse and Mental Health Services Administration (SAMHSA), we have learned that FHIR-enabled C2S APIs provide both physician and patient-facing services and the infrastructure to segment data and manage consent. **We support requiring C2S in Base EHR certification and encourage ONC to increase C2S adoption.** We are also aware that there is no longer funding to continue this important work. **The AMA recommends ONC coordinate with SAMHSA to establish a public-private project to advance C2S.** Vendors and payers have expressed the need to address "the dual challenges of data standardization and easy information access" with the goal "to help payers and providers to positively impact clinical, quality, cost and care management outcomes."[18] We expect health IT vendors and payers would welcome a public-private C2S effort. We recommend an analogous process to that of the Da Vinci Project, but one that is open, transparent, and excludes membership fees. The USCDI and the Interoperability Standards Advisory should be leveraged for support.

Cybersecurity

AMA research has shown that 85 percent of physicians believe it is very important to share electronic health information—they just want to do it safely and within their means.[19] Unfortunately, cyberattacks are inevitable and increasing, leading numerous agencies across the federal government to recognize cybersecurity as a patient safety issue.[20] In fact, the AMA's research revealed that eight in 10 physicians have experienced some form of attack and only 20 percent of small practices have internal security officers despite the fact that 71 percent of ransomware attacks targeted small businesses in 2018.[21,22] Even if a physician's office houses relatively few health care records, it may be connected to other health systems with significantly more data.

These statistics contextualize the security environment in which physicians will need to navigate information blocking requirements. Yet, **ONC's proposals will require physicians to adjust their systems to permit "access", "exchange", and "use" of EHI in new ways—resulting in a series of "trial and error" scenarios and forcing EHR vendors and physicians to guess at what should be accessed or used and from whom.** This could result in exposing multiple entry points to cyber attackers seeking to exploit vulnerabilities, exposing more data than ever before given the amount of information

[18] Health Level 7, Da Vinci Project, available at: http://www.hl7.org/about/davinci/.

[19] AMA, *Patient Safety: The Importance of Cybersecurity in Health Care*, 2018, available at: https://www.ama-assn.org/system/files/2018-10/cybersecurity-health-care-infographic.pdf.

[20] U.S. Food and Drug Administration, FDA News Release, 2018, available at: https://www.fda.gov/news-events/press-announcements/fda-and-dhs-increase-coordination-responses-medical-device-cybersecurity-threats-under-new.

[21] AMA, *Medical Cybersecurity: A Patient Safety Issue*, 2017, available at: https://www.ama-assn.org/delivering-care/patient-support-advocacy/medical-cybersecurity-patient-safety-issue.

[22] Health IT Security, *71% of Ransomware Attacks Targeted Small Businesses in 2018*, March 2019, available at: https://healthitsecurity.com/news/amp/71-of-ransomware-attacks-targeted-small-businesses-in-2018.

ONC is proposing that actors share. These adversaries will target the weakest link in the chain, which may be a physician office or legacy technologies.

ONC's proposals will enable unprecedented electronic access and modification to medical records. Professional societies representing practice administrators, health system chief information officers, and security professionals are already expressing apprehension.[23,24,25] Concerningly, they all sound alarms that EHRs will not sufficiently protect the "use" of EHI as envisioned by ONC. ONC defines *use* in § 171.102 as:

> *the ability of health IT or a user of health IT to access relevant electronic health information; to comprehend the structure, content, and meaning of the information; and to read, write, modify, manipulate, or apply the information to accomplish a desired outcome or to achieve a desired purpose.*

There are major implications for EHI *use* as proposed by ONC. For one, **using EHI would allow an actor (e.g., a consumer-facing app developer) the ability to *read, write,* and *modify* a patient's medical record—including financial, demographic, genetic, protected SUD or mental health, and family information, in an EHR. This is a staggering shift from current EHR capabilities.** Not only are APIs and ONC's proposed API requirements woefully insufficient to protect bi-direction exchange of data, but security experts who participate as HHS advisors have themselves highlighted the need for major security and privacy controls to comply ONC's information blocking proposals.

> *Before enacting the information blocking rule, ONC should first consider selecting or establishing a security controls framework for interoperability and data sharing processes that would support the trusted environments necessary "to build confidence in payers, providers, and patients."*[26,27]

Furthermore, Christopher Wray, the Director of the U.S. Federal Bureau of Investigation (FBI), announced in March 2019 that, "Today's cyberthreat is bigger than any one government agency—in fact it's bigger than the government itself," and that "the scope, breadth, depth, sophistication and diversity of the threat we face now is unlike anything we've had in our lifetimes."[28] These circumstances raise numerous questions:

[23] Health IT Security, *As ONC Considers Info Blocking, IoT, Medical Device Guidance Needed*, April 2019, available at: https://healthitsecurity.com/news/as-onc-considers-info-blocking-iot-medical-device-guidance-needed?eid=CXTEL000000154738&elqCampaignId=9253&elqTrackId=151c5e0bac4b4df6b2155ef6a9ffce20&elq=9d083122ab044763baa6817a857a7474&elqaid=9715&elqat=1&elqCampaignId=9253.

[24] Fierce Healthcare, *Complying with information blocking rule will be a challenge without standardized APIs: HIMSS*, March 2019, available at: https://www.fiercehealthcare.com/tech/complying-information-blocking-rule-will-be-a-challenge-without-standardized-apis-himss.

[25] Health IT Security, *ONC Information Blocking Rule Raises Privacy and Security Concerns*, March 2019, available at: https://healthitsecurity.com/news/onc-information-blocking-rule-raises-privacy-and-security-concerns?eid=CXTEL000000154738&elqCampaignId=8938&elqTrackId=7b46f9fd83434ed99efae92be850fefd&elq=89d147ceb6e246fd99eed1ba66e334b3&elqaid=9402&elqat=1&elqCampaignId=8938.

[26] Id.

[27] CynergisTek is represented on The Healthcare and Public Health Sector Coordinating Council (HSCC).

[28] Healthcare IT News, *RSA 2019: FBI Director Christopher Wray says 'today's cybersecurity threat is bigger than government itself'*, March 2019, available at: https://www.healthcareitnews.com/news/rsa-2019-fbi-director-christopher-wray-says-today%E2%80%99s-cybersecurity-threat-bigger-

- **Has ONC established a security controls framework for interoperability and data sharing?**

- **How will ONC, a single government agency, ensure EHI access, exchange, and use does not compromise the personal health information of U.S. citizens?**

- **What is ONC's plan to ensure that thousands of apps properly authenticate for EHI use?**

- **What is ONC's plan for protecting the multiple access points and attack surfaces that will be necessary to facilitate EHI use?**

- **How is ONC going to ensure EHR vendors develop and test to security industry protective measures, prescribed standards, and security protocols?**

The federal government needs to empower physicians to actively manage their security posture, not hinder them**.** We seek clarity from ONC as to whether it expects physicians to use information blocking exceptions and documentation as "protection" from these risks.

Patients' Trust

Patient privacy is of even greater concern when non-covered HIPAA entities (e.g., consumer facing applications) gain access to medical information. ONC's proposal includes numerous policies that seek to promote application (app) developers' access and use of EHI. One of the strongest comes in the form of API Users and information blocking. The AMA has long heralded the benefit of APIs and apps. Together they can offer better information usability, providing an enhanced view into an EHR's medical record repository. To be clear, **the AMA supports patients' access to their entire record and apps can play an important role.** Yet, **the apps themselves (or app developers) should not be conflated with <u>users of apps</u>.** ONC proposes that the term API User

> *refers to persons and entities that use or create software applications that interact with the APIs developed by the "API Technology Supplier" and deployed by the "API Data Provider." An API User includes, but is not limited to, third-party software developers, developers of software applications used by API Data Providers, patients, health care providers, and payers that use apps/services that connect to API technology.*

We recognize that ONC is attempting to reduce the friction app developers face when trying to connect to EHRs on behalf of patients. This is a legitimate concern. The AMA supports efforts for the seamless integration of apps in EHRs. **However, the AMA has serious concerns that, under ONC's proposed rule, software is being provided equal protections and benefits with those of patients. ONC should refrain from comingling the needs of patients, physicians and other health care providers with those of companies acting adjacent to the provision of care.**

government?mkt_tok=eyJpIjoiTWpjd05HRmtZV0V3WW1OaiIsInQiOiJYN2Q0dVhtQUxHRytncTl1NlZSWXdlekZCSWpMU3hoUmFqZlwvdzBacTBZTjBrR1hWZmlRYWlkc1VpV0RhdE9xWUc5VjF0TDFZNGo2TnV6VG1aZlRndGd6SXRoTFFVWTFUV3Zqdm5YUVNhWUhsSm9ua2tHV1wvTWEwY0hWWHBLN1N1In0%3D.

As proposed, ONC’s EHI and information blocking requirements open the door for apps to access, use, and exchange copious amounts of patient data. Frequently, this will happen without providing patients with clear terms of use. These terms can be 6,000+ words in length, shielding activities such as granting app developers a “royalty-free, perpetual, and irrevocable license, throughout the universe” to “utilize and exploit” their de-identified personal information for scientific research and “marketing purposes.” They may also “sell, lease or lend aggregated Personal Information to third parties”.[29]

A recent Wall Street Journal report exposed just how much is at stake when patients share their personal health information with apps. Several apps were sharing users’ personal health information using Facebook’s technology.[30] A study published in the Journal of the American Medical Association (JAMA) found that many health apps created to track a user’s progress in battling depression or quitting smoking are sharing the personal details they collect about an individual with third parties—like Google and Facebook—without the individual’s knowledge or informed consent:

> Transmission of data to third-party entities was prevalent, occurring in 33 of 36 top-ranked apps (92%) for depression and smoking cessation, but most apps failed to provide transparent disclosure of such practices. Commonly observed issues included the lack of a written privacy policy, the omission of policy text describing third-party transmission (or for such transmissions to be declared in a nonspecific manner), or a failure to describe the legal jurisdictions that would handle data. In a smaller number of cases, data transmissions were observed that were contrary to the stated privacy policies.[31]

Apps are also being used as a powerful monitoring tool for employers and payers. Couched as corporate wellness, employers and payers have aggressively pushed to gather more data about their employees’ lives than ever before.

> Experts worry that companies could use the data to bump up the cost or scale back the coverage of health care benefits, or that women’s intimate information could be exposed in data breaches or security risks. Although the data is made anonymous, experts also fear that the companies could identify women based on information relayed in confidence, particularly in workplaces where few women are pregnant at any given time. [32]

[29] The Washington Post, *Tracking your pregnancy on an app may be more public than you think*, April 2019, available at: https://www.denverpost.com/2019/04/14/tracking-pregnancy-app/.

[30] The Wall Street Journal, *You Give Apps Sensitive Personal Information. Then They Tell Facebook*, February 2019, available at: https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636.

[31] Huckvale K, Torous J, Larsen ME, Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation, JAMA Netw Open. 2019;2(4):e192542. doi:10.1001/jamanetworkopen.2019.2542, available at: https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2730782?utm_source=For_The_Media&utm_medium=referral&utm_campaign=ftm_links&utm_term=041919 .

[32] Id.

This is especially shocking given that hundreds of millions of Facebook user records have been exposed on the Internet.[33] Less than a week after the Wall Street Journal report, another large health system announced the personal information of more than 326,00 patients had been exposed.[34] A Rock Health 2018 National Consumer Health Survey found that just 11 percent of respondents said they would be willing to share health data with tech companies.

In terms of data security, physicians are the most trusted. However, patients are growing extremely concerned about the privacy of their data and believe that sensitive health information is being shared without their knowledge. [35] Specifically, a 2017 Black Book survey reports that:

- 87 percent of patients were unwilling to comprehensively share all their health information with their physicians.
- 89 percent of consumers who had visited a health care provider in 2016 said they had withheld some information during their visits.
- 81 percent were concerned that information about chronic conditions was being shared without their knowledge.
- 99 percent were concerned about the sharing of mental health notes.
- 93 percent of respondents said they were concerned about their personal financial information being shared.[36]

In other words, carelessness and lack of transparency in how consumer information is handled and used by technology has likely influenced what a patient is likely to share with his or her physician. This should serve as a warning to policy makers that consumers take privacy very seriously.

The AMA believes that patients who trust their health systems to protect their data will likely receive better outcomes. Yet, consumer trust is receding. Between 2017 and 2018 patients lost confidence in sharing their health data with the most trusted entities.[37] Patients have a justifiably high expectation of privacy for their electronic health information. As the amount and exchange of health data increases so does the hesitancy for patients to share that information due to privacy and security issues. Losing this trust will lead to serious patient safety issues.[38] It may also weaken our shared goal of achieving value-based care.

[33] Bloomberg, *Millions of Facebook Records Found on Amazon Cloud Servers*, April 2019, available at: https://www.bloomberg.com/news/articles/2019-04-03/millions-of-facebook-records-found-on-amazon-cloud-servers.

[34] Health IT Security, *326,000 Patients Impacted in UConn Health Phishing Attack*, February 2019, available at: https://healthitsecurity.com/news/326000-patients-impacted-in-uconn-health-phishing-attack.

[35] Rock Health, *Beyond Wellness For the Healthy: Digital Health Consumer Adoption 2018*, 2018, available at: https://rockhealth.com/reports/beyond-wellness-for-the-healthy-digital-health-consumer-adoption-2018/.

[36] Black Book, *Healthcare's Digital Divide Widens, Black Book Consumer Survey*, January 2017, available at: https://blackbookmarketresearch.newswire.com/news/healthcares-digital-divide-widens-black-book-consumer-survey-18432252.

[37] Id.

[38] Id.

> *Incomplete medical histories and undisclosed conditions, treatment or medications raises obvious concerns on the reliability and usefulness of patient health data in application of risk based analytics, care plans, modeling, payment reforms, and population health programming.*
>
> *Doug Brown, Black Book Managing Partner*

We need to ensure patients' data are safe, secure, and error-free. Beyond security, we must also maintain the confidentiality and privacy of that data. This should not be viewed as simply good practice. Retaining patient trust and privacy is an ethical consideration.[39] HHS is moving forward on many fronts to empower patients with more control over their own data and allow them to share their information with the provider of their choice. **Any federal proposals that extend access, exchange, or use of EHI must make sure the patient continues to be the primary authority in designating rights to their data.** Cures established the HITAC to set priorities related to electronic health information—specifically noting privacy and security. The HITAC has identified "lack of user awareness and education about privacy and security protections" as a "key gap" in this area and said that there needs to be additional support for patients on these topics.[40] **What is ONC's plan to educate patients about health data privacy and address this key gap?**

ONC should consider a more explicit patient-centered consent framework. It should be straightforward for physicians to administer and give the patient the ability to share their data with another health care institution or a specific practitioner. It should also provide the patient the opportunity to segment some of their data for sharing for a particular period of time. As noted above, we urge ONC to promote these goals through required use of C2S. Under any scenario, the patient must be involved, engaged, and at the center of any decision-making involving the sharing of their personal data.

Patient Empowerment and Control

In addition to constraining ONC's information blocking regulations and interpretation of EHI, ONC should require that all certified APIs include mechanisms to strengthen patients' control over their data. The AMA has heard concerns from consumer groups and patient advocates about the volume, variety, and velocity of data that will be shared without assurances of privacy and security. We again reiterate that patients should have complete access to their data. HIPAA reinforces this right. The AMA believes that patients are just as interested in protecting their data's privacy as they are in accessing it. As previously discussed, the complex set of regulatory unknowns may encourage oversharing or unfettered access and use. Indeed, many companies are well-positioned to benefit from the proposed rule.

In reading the proposals, we also question the level of deference provided to entities seeking to commoditize patient data. Information that is collected has been likened to a "digital tattoo" that is impossible to expunge.[41] The Equifax hack in 2017 exposed nearly 148 million individuals'

[39] TechCrunch, *Demanding privacy, and establishing trust, in digital health*, March 2019, available at: https://techcrunch.com/2019/03/26/demanding-privacy-and-establishing-trust-in-digital-health/amp/

[40] ONC, *HITAC Annual Report for Fiscal Year 2018 Executive Summary*, March 2019, available at: https://www.healthit.gov/sites/default/files/facas/2019-03-19%20HITAC%20Draft%20Annual%20Report%20-%20Executive%20Summary%20Handout.pdf

[41] The New York Times, *We're Not Going to Take It Anymore*, April 2019, available at: https://www.nytimes.com/2019/04/10/opinion/internet-privacy-regulation.html#click=https://t.co/XvdMfPlIBv

information.[42] Equifax is considered by many as a credit reporting agency. However, its activities as a data broker generate significant profit.[43] The data "buying and selling" ecosystem is increasingly intertwined—making it more likely the patient information will be *traded* not just exchanged. For example, recent reports note the ability of even innocuous-seeming gaming apps to glean and monetize revealing user data:

> *The intricacies of gameplay data can tell you a lot about what makes people tick, and what's going on with them — studies have shown that you play games differently when you're depressed, or dieting. "Nobody gets too upset about games," Nieborg says. "But the underlying technology is really powerful. These people are really pushing the technology to the limits where the potential for abuse is massive."*
>
> *"There's a massive incentive to know a lot about your players," he says, and the "dark twist" is that "If you can do this for a games company and you're really good at it, you can [then go] start working for other companies that have less trivial goals than just selling digital gems to people."*[44]

The data leak is not limited to gaming information. Apps, particularly free apps, often use advertisements to generate revenue. The advertisements collect and share an individual's advertising ID—a string of numbers and letters that identify an individual and keep a log of his or her clicks, searches, purchases, and sometimes geographic location as he or she moves through various apps.[45] While the information is often deemed anonymous, the information can be "shockingly easy to de-anonymize, and that hundreds of apps collect 'anonymous' real-time location data that needs only the slimmest additional context clues to tie to an individual person."[46] **If ONC prioritizes making patients the center of their care, and states that patient access to data on their smartphones will enable this, what is ONC doing to ensure that patients do not become products?**

We also note that Draft 2 of the Trusted Exchange Framework and Common Agreement (TEFCA) specifically raises concerns with non-HIPAA entities' use of electronic health information.

> Individuals, health care providers, health plans, and networks may not be willing to exchange data through the Common Agreement if smartphone app developers and other non-HIPAA entities present privacy or security risks because they are not obligated to abide by the HIPAA Rules. In order to meet the goals of the Cures Act as well as to help address these concerns and encourage robust data exchange that will ultimately improve the health of patients, the Common Agreement requires non-HIPAA entities, who elect to participate in exchange, to be bound by certain provisions that align with safeguards of the HIPAA Rules. This will bolster

[42] Money, *The Equifax Hack Affects 143 Million People. Here's What Makes It Even Worse*, September 2017, available at: http://money.com/money/4933204/equifax-hack-credit-report-identity-theft/?iid=sr-link7

[43] Fast Company, *Here are the data brokers quietly buying and selling your personal information*, March 2019, available at: https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information

[44] Vox Media Network, *Angry Birds and the end of privacy*, May 2019, available at: https://www.vox.com/explainers/2019/5/7/18273355/angry-birds-phone-games-data-collection-candy-crush

[45] Id.

[46] Id.

> data integrity, confidentiality, and security, which is necessary given the evolving cybersecurity threat landscape.[47]

We are confused by the dichotomy between ONC's proposed rule and the clear concern outlined in the TEFCA. ONC should ensure its multiple proposals and regulations are aligned with patient privacy and app developer requirements.

If patients access their health data—some of which could contain family history and could be sensitive—through a smartphone, they must have a clear understanding of the potential uses of that data by app developers. Most patients will not be aware of who has access to their medical information, how and why they received it, and how it is being used (for example, an app may collect or use information for its own purposes, such as an insurer using health information to limit/exclude coverage for certain services, or may sell information to clients such as to an employer or a landlord). The downstream consequences of data being used in this way may ultimately erode a patient's privacy and willingness to disclose information to his or her physician. ONC's proposal requires API usage without requiring that the API technology include privacy controls. **The technological capability to implement privacy controls exists, so by failing to implement them, the agency is making a deliberate policy decision to not prioritize privacy.**

To assist in resolving this issue, the AMA has identified an opportunity for multiple coexisting components to empower patients with meaningful knowledge and control over the use of their data. We believe that ONC has the responsibility to provide patients with a basic level of privacy and app transparency—especially since some apps deliberately hide their actions and make it difficult for patients to learn about or control their data. The AMA urges ONC to take the following steps to ensure patient data are accessed, exchanged, and used pursuant with the goals outlined in Cures and the desires expressed by patients.

As part of an API Technology Supplier's certification, **ONC should require APIs check an app's attestation to:**

- **Industry-recognized development guidance;**
- **Transparency statements and best practices; and**
- **The adoption of a model notice to patients.**

One possible method to accommodate this would require an EHR vendor's API to check for three "yes/no" attestations from any consumer-facing app. For example: 1) An app developer could choose to assert conformance to Xcertia's Privacy Guidelines. [48] 2) An app developer could attest to the Federal Trade Commission's (FTC) Mobile Health App Developers: FTC Best Practices and the CARIN Alliance Code of Conduct. 3) An app developer could attest to adopting and implementing ONC's Model Privacy Notice. These could be viewed as value-add services as proposed by ONC. The app could be

[47] ONC, *Trusted Exchange Framework and Common Agreement (TEFCA) Draft 2*, 2019, available at: https://www.healthit.gov/sites/default/files/page/2019-04/FINALTEFCAQTF41719508version.pdf.

[48] Both the Food and Drug Administration (FDA) and ONC participate on the board of Xcertia, a multi-stakeholder effort to develop guidelines and recommendations for medical app development.

acknowledged or listed by the health IT developer in some special manner (e.g., in an "app store," "verified app" list). We would urge EHR vendors to also publicize the app developers' attestations; ONC could also require a vendor to do so as a prerequisite to product certification.

We do not believe that requiring an API check for an app developer attestation would be a significant burden on API Technology Suppliers. We recognize that a "yes" attestation would not ensure apps implement or conform to their attestations. However, we firmly believe this will provide a needed level of assurance to patients and would be greatly welcomed by users. **We also believe this could act as a "bookend"—placing app developers between ONC health IT certification requirements (which would be imposed by API Technology Suppliers), and FTC's enforcement of unfair and deceptive practices. In other words, an app developer would be strongly motivated to attests "yes" and to act in line with their attestations.**

We are aware there are some who believe requiring this minimum level of privacy controls for patients is "paternalistic." This characterization is perplexing given that patient privacy is a fundamental aspect of Cures, necessary for patients to safeguard themselves from data profiteering and discrimination, and promoted by the AMA Code of Medical Ethics and House of Delegates which includes representation from state and territorial medical associations, national medical specialty organizations, and the federal government. As noted above, one of the purposes of Cures is to provide individuals with access to their health information without special effort. Most consumers would probably characterize multiple pages' worth of privacy practices, which may or may not be transparent, as requiring special effort. So why does the agency charged with implementing Cures dismiss concern over patient privacy with a "buyer beware" mentality? It is alarming that ONC appears to view its charge as merely providing access to data, and not meaningfully empowering the patient as the spirit of Cures intended.

The Practicality of Proposed Regulations

There are many questions around the ability of actors to comply with information blocking regulations in light of ONC's proposed EHI definition. Many of these spur from the nebulous nature of what could be considered EHI. ONC proposes EHI to mean:

- electronic protected health information; and

- (ii) any other information that –
  - is transmitted by or maintained in electronic media, as defined in 45 CFR § 160.103;
  - identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual; and
  - relates to the past, present, or future health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

ONC states that this definition provides for an expansive set of EHI. It could include information on an individual's health insurance eligibility and benefits, billing for health care services, and payment information for services to be provided or already provided, which may include price information. EHI may also be provided directly from an individual, or from technology that the individual has elected to use, to an actor covered by the information blocking provisions. In addition, ONC's definition of interoperability elements is very broad—going beyond certified health IT—and interacts with the identified information blocking practices and actors, along with other aspects of the information blocking requirements, to create a very broad and complex web of compliance risk.

Furthermore, ONC's examples of what would constitute information blocking, the wide net cast by the definition of "actors", the complexity of knowing when an interoperability exception would apply, plus the added ramifications for physicians to navigate HIPAA "minimum necessary", designated record sets, and electronic protected health information (ePHI) while at the same time ensuring Privacy and Security Rule requirements are adhered to is overwhelming. **We remind ONC that section 4001 of Cures establishes a goal with respect to the reduction of regulatory or administrative burdens. We again highlight multiple Cures provisions create a narrative, and when read together, tell a cohesive story.** The AMA has identified a set of corrective actions ONC should take to help ameliorate the complexities.

Align information blocking with the USCDI

The AMA has identified several instances where the proposed information blocking and EHI regulations will create unintended consequences for everyone involved. It is already causing confusion among those explicitly included as "actors;" it will also cause companies, groups, and individuals who have not contemplated involvement to question if they, too, are actors. This issue has raised the attention of the Congressional representatives who authored Cures.

Additionally, we have concerns with HHS' ability to administer regulations as proposed. ONC has already postponed its regulatory promulgation of a Cures provision (i.e., EHR Reporting Program) due to financial limitations. The challenges posed to privacy and security in the near-term are far too large for ONC to handle on its own; these challenges likely are beyond the scope of HHS, and even the current statutory authority of the whole Executive Branch, to address adequately.

Furthermore, we foresee situations where actors will utilize their "legal prowess" to enforce their will on other actors. For instance, a small physician's practice will not have the resources to translate regulation, institute comprehensive policy and procedures, and defend against information blocking threats from large health systems, payers, or consumer-facing app developers. Even if an EHR vendor is the culprit for information blocking, a small practice would have little leverage against a multi-billion-dollar company. We are concerned how this would impact independent, solo, and rural medical practices across the nation.

We also note the state of health care interoperability today and how difficult it is to exchange data—even if it is electronic—if it is not structured. Physicians continue to rely on the fax machine to exchange even the most basic pieces of information. By expanding that universe to all EHI, we will only exacerbate the current problem of exchanging unusable data in burdensome ways with minimal return.

The AMA has identified a more pragmatic approach to information blocking and EHI and discussed it with several stakeholders—representing hospitals, EHR vendors, professional associations, health information exchanges, and patients. **There is a consensus that information blocking should be aligned with the USCDI.** There is common agreement that the USCDI does not constitute the entirety of every actors' requirements. Physicians and patients may request information beyond the USCDI. The USCDI is also not sufficient to accomplish ONC's proposed EHI export requirement. However, there are several reasons we believe the USCDI is a practical starting point to encourage greater information sharing and use while supporting privacy, security, and feasibility concerns.

- ONC is proposing major changes to health IT certification, particularly around APIs, testing, Conditions of Certification/Maintenance of Certification, and fees all associated with the USCDI. **The AMA greatly appreciates many of these proposals and agrees certification should focus on consistently applied implementation guides and tested standards.** Certified APIs and the USCDI can provide a framework to strengthen privacy (e.g., API attestation check). Security can be strengthened by consistently applying OpenID Connect and OAuth 2.0 protocols and scoping regulations to read access only. Advancing the FHIR standard, including ONC's proposals to create the ARCH between the USCDI and FHIR Resources, will further the usability of data. Additionally, the USCDI will be expanded over time—proving an opportunity to respond to patient and physician data needs in a structured way. Complementarity processes, such as the Interoperability Standards Advisory (ISA) and the proposed Standards Version Advancement Process (SVAP), will bolster the USCDI to support access, use, and exchange of electronic health information.

- The Centers for Medicare & Medicaid Services' (CMS) proposed interoperability and patient access rule focuses on the access, use, and exchange of the USCDI. CMS provides several reasons why the USCDI is an appropriate standard to facilitate care coordination without burdening stakeholders—outlined below. ONC should also consider the potential dichotomy with EHI information blocking and other HHS regulations.

> We are proposing a new requirement for Medicare Advantage (MA) plans, Medicaid managed care plans, CHIP managed care entities, and QHPs in the FFEs to require these plans to maintain a process to coordinate care between plans by exchanging, at a minimum, the USCDI at enrollee request at the specific times specified in the proposed regulation text…. The USCDI (Version 1) data set would have to be sent to another plan that covers the enrollee or a recipient identified by the enrollee at any time during coverage or up to 5 years after coverage ends, and the plan would have to receive the USCDI (version 1) data set from any health plan that covered the enrollee within the preceding 5 years.
>
> We believe that exchanging this [USCDI] minimum data would help both plan enrollees and health care providers coordinate care and reduce administrative burden to ensure that plans provide coordinated high-quality care in an efficient and cost-effective way that protects program integrity. Leveraging interoperability to facilitate care coordination among plans can, with thoughtful execution, significantly reduce unnecessary care, as well as ensure that health care providers are able to spend their time providing care rather than performing unnecessary administrative tasks. We believe that use of the USCDI to exchange information furthers care coordination… This addresses concerns stakeholders have previously raised with CMS and ONC regarding such administrative burdens, as the USCDI standard contains many of the data points required to more effectively coordinate care…. The USCDI (Version 1) data set includes laboratory results and tests, medications, health concerns, assessment and plan of treatment, care teams, clinical notes, and other data points essential for care coordination. This would provide the patient with a

> more comprehensive history of their medical care, helping them to make better informed health care decisions.
>
> …These data exchanges would provide the enrollee's new plan with a core set of data that can be used to support better care coordination and improved outcomes for the enrollee. We considered requiring plans to exchange all the data that we proposed be available through an API (see section III. of this proposed rule) but we understand that ingesting data and reconciling errors has challenges and proposed this more limited data set to address those concerns… Many key attributes of the USCDI make it suitable for the purpose outlined in our proposal. The USCDI includes data classes that can be supported by commonly used standards, including the Health Level Seven (HL7) Consolidated Clinical Data Architecture (C–CDA) Version 2.1 and the Fast Healthcare Interoperability Resources (FHIR) standards for essential patient health information like vital signs, lab results, medications and medication allergies. The USCDI establishes a minimum set of data elements that would be required to be interoperable nationwide and is designed to be expanded in an iterative and predictable way over time. The USCDI, at a minimum, transferred for each enrollee moving among the plans subject to our proposal would greatly improve each plan's coordination of care efforts and spotlight areas of urgent need. [49]

- Without aligning information blocking and EHI with the USCDI, ONC may inadvertently establish divergent expectations between certified health IT and the access, use, and exchange of EHI. EHR vendors will be expected to comport with API and USCDI certification requirements. This will be a major undertaking by many EHR vendors, particularly those that serve medical specialists as they are typically smaller companies providing specific tools to physicians. ONC is proposing that EHR vendors make these changes within 24 months of the final rule's effective date. However, ONC is also proposing actors, including physicians and EHR vendors, comply with information blocking and EHI requirements starting on the effective date of the final rule. This creates a federal mandate that many will not be able to comply with—akin to mandating that water flow from a spigot before the plumbing is connected.

We encourage ONC to establish a more unified interoperable infrastructure so that patients can safely and securely access their medical records using the app of their choice. Many of these apps are already being developed to support the USCDI data elements. Coordinating efforts around the USCDI and APIs will provide more value for patients than a bulk dump of unstructured data. Apps should be able to get data from an EHR through known protocols and standards—providing an easy-to-use and easy-to-understand cohesive data set. Policy efforts should promote technical requirements to deliver a defined concept of EHI to patients in a computable format so that their data can be used once made available. It is likely that an EHR will have multiple APIs, each connecting to a different service. We expect EHR vendors will eventually establish an orchestration of secure API services to facilitate access and use to the complete medical record. **ONC should encourage this approach by promoting the USCDI as a logical interoperability building block.**

[49] CMS, 45 CFR Part 156, [CMS–9115–P], RIN 0938–AT79, March 2019, available at: https://www.govinfo.gov/content/pkg/FR-2019-03-04/pdf/2019-02200.pdf.

Alignment between ONC's information blocking, EHI, and USCDI proposals could happen in several ways. The AMA is recommending two potential paths:

- ONC could constrain its definition of EHI to just the data elements represented by the USCDI for specified actors. Information blocking requirements would be subject to newly-scoped access, use, and exchange of the USCDI. Patients would retain their rights to request their designated record set as outlined by HIPAA (the Director of the HHS Office of Civil Rights has already noted publicly that patient access enforcement will increase this year). EHI export could be scoped to focus on ePHI as outlined by HIPAA. Additional data classes (e.g., payment and cost information) would propagate through the USCDI expansion process with support from the ISA and SVAP.

- Alternatively, ONC could retain its EHI definition, rescope the terms "access," "use," and "exchange," and include additional information blocking exceptions. ONC could establish an exception for actors only able to make the USCDI available. This exception should be concise, clear, implementable, and refrain from burdensome policy and procedure requirements. This could also be accomplished by modifying the proposed "Infeasibility of Request" exception. We encourage ONC to clarify that actors that do not comply with the request for access, exchange, or use of EHI, but that do comply to the best of their ability with requests for access, exchange, or use of the USCDI be able to claim this exception. Also, ONC should clarify that an actor could claim an exception for responding in "good faith" to requests beyond the USCDI.

Limit Subjective Language

The AMA has concern with ONC's interpretation of Health Information Networks (HINs) and Interoperability Element.

The proposed Part 171 Information Blocking contains definitions for terms such as electronic health information, information blocking, access, use, and exchange that are used throughout Part 171. These terms are also used in proposed provisions in Part 170; however, Part 170 does not define these terms. As proposed, this lack of definitions creates the ability to have two separate interpretations of these terms depending on which part and introduces unnecessary vagueness and inconsistency. ONC could remedy this situation by defining these terms in Part 170 with regulatory language such as "is defined as it is in §171.102 of this subchapter." However, ONC should be aware of any potential unintended consequences in applying these terms throughout Part 170. For example, with the proposed definition "use" having writing capability being extended to CEHRT requirements.

The AMA strongly recommends that the definition of HIN be narrowed to include only entities that are an actual network (or formalized component of an actual network) and have an actual operational role and responsibility for the network. For example, to be a HIN, the network itself provides the ability to locate and transmit EHI between multiple persons and/or entities electronically, on demand, or pursuant to one or more automated processes. Moreover, to be a HIN, the entity should also be exchanging EHI in a live clinical environment using the network in some capacity. Thus, health care providers and organizations with limited exchange capabilities, such as interfaces for Admission, Discharge, and Transfer messages or lab results, should not be considered a HIN.

HINs typically operate as Business Associates and currently have Business Associate agreements in place with their participants who are Covered Entities. These agreements facilitate the exchange of EHI since they perform functions or activities on behalf of or provide certain services for Covered Entities such as determining and administering policies or agreements that define business, operational, technical, or other conditions or requirements for enabling or facilitating access, exchange, or use of health information between or among two or more Covered Entities. Therefore, for example, organizations that develop voluntary standards and policies that may be used by a HIN should not be considered a HIN.

In defining "Interoperability Element", ONC states that the term is not limited to functional elements and technical information but also encompasses technologies, services, policies, and other conditions necessary to support the uses of EHI. ONC's intent is to capture the potential means by which EHI may be accessed, exchanged, and used. **The AMA believes that Interoperability Element should not include the underlying substantive content because such content is not a potential means by which EHI may be accessed, exchanged, or used. Therefore, ONC should clarify that underlying substantive content is not included in the definition of Interoperability Element.**

Separate Development and Adoption Timelines

ONC is proposing several changes to its certification program, including §170.315(g)(10)-APIs, EHI export, USCDI adoption, Real World Testing, Standards Version Advancement Process, Communications, and Assurances. The AMA appreciates ONC responding to our advocacy on these issues. As previously stated, EHR vendors will require a considerable amount of time to make changes and comply with Conditions and Maintenance of Certification. 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 final rule's effective date. Because most physicians 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 <u>and</u> physician EHR adoption, implementation, and use concurrently.** Not only does this create an incredibly ambitious timeline, it also effectively usurps CMS' authority to determine when physicians use a particular CEHRT requirements for incentive program participation.

EHR developers should be provided a specific timeline to develop, test, certify, publish, implement, and train their customers on new product features and functions. This timeline should be separate from physician adoption requirements, which is squarely in CMS' purview. While we support a two-year time horizon for development, implementation, and go-live, we do not support ONC dictating the adoption schedule for physicians. If ONC continues with its proposal it should, at the very least, provide physicians additional time beyond 24 months. Once our members have entered into their vendor's implementation queue, they continue to experience 12+ month timelines before EHRs are upgraded/installed. We reiterate that ONC should remain focused on the technology, while other HHS agencies and offices dictate adoption policies. We also caution ONC against using language that implies that both certified health IT developers and their customers are required to meet the 24-month timeline (e.g., health IT developers "must provide all of its customers…"); this wording extends ONC's regulatory reach beyond health IT developers to providers. Rather, ONC should require that health IT developers "make available" to its customers upgraded product features and functions within 24 months.

For this reason and to prevent significant confusion for physicians about program requirements, the AMA strongly recommends ONC refrain from adjusting the 2015 Edition Base EHR definition.

We do not agree with ONC's reasoning to not propose 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 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.

Reduce Administrative Burden

The AMA is concerned about the potential increase of administrative burden the proposed rule places on the practice of medicine. The AMA also opposes any unfunded mandates. The increasing amount of administrative responsibility forced upon physicians adds unnecessary costs not only to physicians but also to patients. Unnecessary administrative tasks undercut the patient-physician relationship. The increase in administrative tasks is unsustainable, diverts time and focus away from patient care, and leads to additional stress and burnout among physicians.

Through Executive Order, ONC is required to manage the costs associated with the governmental imposition of private expenditures required to comply with federal regulations.[50] Moreover, given the burden and cost, the AMA is concerned that the proposed rule will lead to further consolidation of the health care market, increase barriers of entry for new practices, and exasperate the abuses of market power.[51] The AMA believes ONC can manage these costs and reduce the amount of administrative burden placed upon physicians in this proposed rule, while also simplifying the health care system and ensuring patients receive access to their health information. By streamlining the administrative burden in this proposed rule, ONC can support the patient-physician relationship and let physicians focus on an individual patient's welfare and, more broadly, on protecting public health.

Thus, AMA makes numerous recommendations throughout this proposed rule that, in part, help simplify the reporting, monitoring, and documentation requirements:

- Aligning information blocking, EHI, and USCDI proposals;
- Creating a separate timeframe for physician implementation of the new CEHRT requirements;
- Streamlining the fee structure;
- Clarifying that a physician's professional judgment to protect their patients' privacy rights is never considered to be information blocking;
- Clarifying that a physician providing the minimum necessary information to an actor will not be considered an information blocker;
- Limiting subjective language in the definitions involving information blocking and the new CEHRT requirements; and
- Requiring the adoption of FHIR Release 4.

[50] Executive Order 13771, Reducing Regulation and Controlling Regulatory Costs (Jan. 30, 2017).
[51] Executive Order 13813, Promoting Healthcare Choice and Competition Across the United States (Oct. 12, 2017).

Supplemental Notice of Proposed Rulemaking

The AMA also recommends that ONC consider issuing a Supplemental Notice of Proposed Rulemaking (SNPRM) to seek further comments on the information blocking provisions the proposed rule. We applaud Congress' intent in section 4004 of the Cures Act to eradicate practices that unreasonably limit the access, exchange and use of electronic health information for authorized and permitted purposes which in turn have frustrated care coordination and improvements in health care quality and efficiency as well as inhibited the transition to a learning health system. That said, Part 171 of the proposed rule introduces a number of new definitions and terminologies, including such definitions as "electronic health information," "use," and "health information network" that require additional clarification from ONC before the entire rule is finalized given the significant economic impact of this rule. Furthermore, a number of regulatory and deregulatory actions on the Office of Management and Budget's Unified Agenda await regulatory action, including changes to the 42 CFR Part 2 regulation, potential modernization of HIPAA to support and remove barriers to coordinated care, as well as enactment of TEFCA, all of which have immediate implications for Part 171 of this proposed rule.

Moreover, ONC is requiring physicians comply with all detailed and complex information blocking provisions without knowing the potential appropriate disincentives. ONC deferred to future rulemaking as to the potential penalties for physicians. Thus, asking physicians to comply with an unfunded mandate without knowing the penalties is unfair. It is not our intent to slow ONC's implementation of Title IV of the Cures Act as mandated by Congress. However, issuance of an SNPRM would enable ONC to propose additional clarifications to the information blocking rule and seek feedback on its proposals to address identified concerns before finalizing the information blocking section of this proposed rule. We also believe that issuance of a SNPRM would provide ONC with the desired flexibility, if it so chooses, to finalize certain aspects of the rule while concurrently issuing a SNPRM on Part 171.

Should ONC choose not to issue a SNPRM, ONC should extend the effective date of the final rule by at least six months in order for physicians to have the necessary time to fully digest and implement changes in their business practices, policies, and procedures. This is necessary to help physicians and patients fully understand the implications of the Administration's policies and ensure actors have time to seek clarifying feedback from HHS' agencies on myriad questions without fear of penalties.

The AMA shares the Administration's continued focus on improving interoperability and patient access across the U.S. We look forward to continuing our work with the Administration to secure long-lasting revisions to health IT policy and implement Cures provisions. Physicians and patients must be provided better access to needed clinical information while at the same time being assured privacy and security are strengthened. If you have any questions, please feel free to contact Matt Reid, Assistant Director, Federal Affairs, at matt.reid@ama-assn.org or 202-789-7419.

Sincerely,

James L. Madara, MD

Office of the National Coordinator for Health IT Proposed Rule Public Comment Template

21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program

Preface

This public comment template supports a specific proposed rule that would implement certain provisions of the 21st Century Cures Act. The template is not intended to substitute for review of the 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program proposed rule published in the *Federal Register* at 84 FR 7424. A PDF copy of the official version of the rule is available from the FederalRegister.gov website at https://www.govinfo.gov/content/pkg/FR-2019-03-04/pdf/2019-02224.pdf.

This template is intended to provide a simple way to organize and present comments on the new and modified provisions in 45 CFR Parts 170 and 171, and responses to specific questions posed in the preamble of the proposed rule. While use of this document is entirely voluntary, commenters may find it helpful to use the document in lieu of unstructured comments, or to use it as an addendum to narrative cover pages.

To further enhance the public comment experience, in complement to this public comment template, an unofficial copy of the proposed rule is also available in Microsoft Word format on ONC's website at https://www.healthit.gov/sites/default/files/page/2019-03/ONCCuresActProposedRule.docx. We believe having a copy of the rule available in Microsoft Word will make it easier for commenters to access and copy portions of the proposed rule for use in their individual comments.

The following tables are organized according to the table of contents of the proposed rule, and the order in which proposed new and revised provisions are discussed in the preamble of the rule rather than the order in which the proposals would be codified in regulatory text. Tables pertaining to proposals include the *Federal Register* page(s) of the proposed rule where the regulatory impact analysis related to the proposal can be found. All tables include the *Federal Register* page(s) of the proposed rule where the preamble discussion of the proposal can be found. Each table provides a field for submitting comments on the proposals or requests for information, including, but not limited to, responses to specific questions or requests for comment posed in the preamble. This field can be expanded as necessary for commenting.

To be considered, all comments (including comments organized using this document) must be submitted according to the instructions in the proposed rule. Electronic submissions are strongly encouraged and can be easily completed through the regulations.gov website (The proposed rule's docket is at https://www.regulations.gov/document?D=HHS-ONC-2019-0002-0001). Look for the "Comment Now" button on the upper right.

21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program

Section III – Deregulatory Actions for Previous Rulemakings

Removal of Randomized Surveillance Requirements

We propose to revise § 170.556(c) by changing the requirement that ONC-Authorized Certification Bodies (ONC-ACBs) must conduct in-the-field, randomized surveillance to specify that ONC-ACBs may conduct in-the-field, randomized surveillance.

We further propose to remove the following:

- The specification that ONC-ACBs must conduct randomized surveillance for a minimum of 2% of certified health IT products per year.
- Requirements regarding the exclusion and exhaustion of selected locations for randomized surveillance.
- Requirements regarding the consecutive selection of certified health IT for randomized surveillance.

Without these regulatory requirements, ONC-ACBs would still be required to perform reactive surveillance, and would be permitted to conduct randomized surveillance of their own accord, using the methodology identified by ONC with respect to scope and selection method, and the number and types of locations for in-the-field surveillance.

Preamble FR Citation: 84 FR 7434 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Please see 84 FR 7562-63 for estimates related to the removal of randomized surveillance requirements.

Public Comment Field:

The AMA supports the removal of randomized surveillance because new and more detailed conditions and maintenance of certification requirements have been proposed. We highlight that removal may increase physician responsibility to flag certification issues. ONC should develop additional education and guidance to help physicians know what would be considered in and out of conformance with certification.

We also worry that, since ONC has not chosen to implement Cures' EHR Reporting Program provision, physicians will not have a "go-to" resource to report or learn about EHR issues. We recommend that ONC direct ONC-ACBs to engage in reactive surveillance when users report usability, safety, security, privacy, or interoperability concerns openly (e.g., as described by Cures § 4002. Transparent reporting on usability, security, and functionality).

Removal of the 2014 Edition from the Code of Federal Regulations

We propose to remove the 2014 Edition certification criteria (§ 170.314) and related standards, terms, and requirements from the rule.

Preamble FR Citation: 84 FR 7434-35

Specific questions in preamble? *No*

Regulatory Impact Analysis: Please see 84 FR 7563-64 for estimates related to the removal of the 2014 Edition from the Code of Federal Regulations.

Public Comment Field:

The AMA supports removal of the identified criteria and standards from 2015 Edition criteria for the reasons articulated by ONC and because CMS removed requirements to use some of these listed criteria.

We disagree with ONC reasoning to not propose a new Edition designation. We question why ONC proposed to modify the 2015 Edition as opposed to creating a new Edition. ONC is proposing broad-sweeping changes to the 2015 Edition. By not updating to a new Edition, users of the Certified Health IT Product List (CHPL) will be confused about which version of 2015 Edition is being referenced. ONC should release a new Edition given the substantial changes being proposed. We recommend a 2020 Edition or the corresponding year in which this rule is finalized. HHS should direct its agencies to update regulations to reflect the new Edition.

Removal of Certain 2015 Edition Certification Criteria

We propose to remove certain certification criteria, including criteria that are and are not currently included in the 2015 Edition Base EHR definition at §170.102.

We propose to remove from § 170.315 and § 170.102 the following 2015 Edition Criteria that are currently included in the 2015 Edition Base EHR definition:

- "problem list"
- "medication list"
- "medication allergy list"
- "drug formulary and preferred drug list checks"
- "smoking status"

We also propose to remove from § 170.315 the following 2015 Edition certification criteria that are not included in the 2015 Edition Base EHR definition:

- Patient-specific education resources
- Common Clinical Data Set Summary (CCDS) Record – Create
- Common Clinical Data Set Summary (CCDS) Record – Receive
- Secure Messaging

Preamble FR Citation: 84 FR 7435-37 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Please see 84 FR 7565-66 for estimates related to the removal of certain 2015 Edition certification criteria and standards.

Public Comment Field:

The AMA disagrees with ONC's proposal to remove from the 2015 Edition Criteria the problem list, medication list, medication allergy list, drug formulary, and smoking status requirements. EHR vendors must be required continue to support these requirements especially with the Tobacco Use: Screening and Cessation Intervention measure. This measure has recently changed from recording all patients screened regardless of tobacco use to just patients who screen positive for smoking and measuring cessation intervention at each patient encounter. Measure 226 is the second most commonly reported measure in the Merit-based Incentive Payment System (MIPS) by eligible clinicians across all quality reporting mechanisms including CMS Web Interface. Based on the 2017 Quality Payment Program (QPP) Experience Report, close to 500,000 eligible clinicians selected this measure in the first performance year.

Moreover, the AMA recommends ONC remove barriers limiting Systematized Nomenclature of Medicine (SNOMED) categories for smoking status. We note that documentation mechanisms in EHRs do not account for length and duration of smoking and that any simplification of the current SNOMED codes could have unforeseen consequences and impacts. We believe addressing SNOMED code limitations will improve EHR usability and help reduce smoking.

Furthermore, ONC should coordinate with measure stewards, including national medical societies, on the development of future quality measures. Medical specialties should not be required to dilute measure development due to delinquencies in EHR data capture.

Removal of Certain ONC Health IT Certification Program Requirements

We propose to remove the following ONC Health IT Certification Program requirements at § 170.523:

- Limitations disclosures
- Transparency and mandatory disclosures requirements

Preamble FR Citation: 84 FR 7437-38 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Please see 84 FR 7566-67 for estimates related to this proposal.

Public Comment Field:

The AMA supports ONC's proposal to, as a complementary Condition of Certification, prohibit developers from taking any action that could interfere with a user's ability to access or use certified capabilities for any purpose within the scope of the technology's certification.

We do not support ONC's proposal to remove Principles of Proper Conduct (PoPC) in § 170.523(k)(2) which requires health IT developers to submit an attestation validating compliance with mandatory disclosure requirements. ONC reasons it is no longer necessary since health IT developers are readily complying with the requirements. However, our experience is that PoPC requirements are themselves the motivating factor and therefore should continue to be enforced. We recognize the need to reduce burden, but an attestation (which ties a developer to their actions) is not burdensome. Additionally, ONC should refrain from actions that reduce transparency. At a time when the Administration is calling for more transparency across the health care continuum, we find it perplexing that ONC is proposing to remove a key transparency requirement from EHR vendors.

Recognition of Food and Drug Administration Processes

We propose to establish processes that would provide health IT developers that can document successful certification under the Food and Drug Administration (FDA) Software Pre-Certification Pilot Program with exemptions to the ONC Health IT Certification Programs requirements for testing and certification of its health IT to the 2015 Edition "quality management systems" criterion and the 2015 Edition "safety-enhanced design" criterion, as these criteria are applicable to the health IT developer's health IT presented for certification. We also believe that such a "recognition" could be applicable to the functionally-based 2015 Edition ''clinical'' certification criteria.

Preamble FR Citation: 84 FR 7438-39 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Not Applicable

Public Comment Field:

The FDA's Pre-Certification Program is a risk-based regulatory framework to facilitate software as a medical device (SaMD). We understand the volume and rapid-cycle iterative improvements in SaMD dictate a new approach that would allow the FDA to streamline oversight for lower risk products while allocating scarce resources to the highest risk regulated digital health tools. The AMA notes that a confluence of factors is driving the need to develop alternative options for regulatory oversight of SaMD, including the rapid iterations in SaMD, the capability of SaMD supporting technologies to track post-market impact, and the proliferation of SaMD which is outpacing regulatory agency capacity to review and surveil.

However, we note that health IT development and use should not be conflated with SaMD. Congress specifically carved many health IT components out of FDA's jurisdiction (e.g., EHRs). The FDA has pivoted from what most would consider "traditional health IT" to other aspects of digital health (e.g., SaMD, Artificial Intelligence (AI), digital therapeutics). This is not to say EHR development will not eventually incorporate AI or other technologies that intersect with the FDA. However, the Pre-Certification Program is still early in its first full year of operation, having received SaMD technology applications by way of its pilot participants. We note that none of the pilot participants are considered EHR vendors. As such, we do not believe the FDA has contemplated the full picture of EHR user needs in Pre-Certification, nor has the Pre-Certification Program experienced applicants representing EHR vendors or their users' interests.

We also have concerns with the potential for entities to get "certified" to ONC health IT requirements when they have not first had experience going through ONC's certification testing process. FDA's Pre-Certification Program specifies that a business unit or business center—not the actual product or application—is granted precertification status. Organizations that have not successfully deployed certified EHR products (CEHRT) should first demonstrate that they are able to deploy such software safely through ONC's existing oversight process. Circumventing this process would degrade trust in ONC's oversight and would fail to provide a documented track record of performance or accountability.

We do not agree that the FDA's Pre-Certification Program (and/or subsequent finalized program) sufficiently aligns with ONC's Program. We further do not believe ONC could properly operationalize an ONC/FDA-hybrid approach and ensure certifications indicate which criteria have been "deemed certified" by ONC, but still subject to ONC-ACB surveillance. We believe focusing on whether a company or organization excels in software design, development, and validation (testing) are important components. We also believe that the track record of the developer's products is equally important; thus, post-market active sentinel capabilities with organized feedback loops—easily captured by regulators as well as developers—are essential. ONC's current program and proposed changes to Conditions of Certification and Maintenance of Certification, while not perfect, are better facilitators of real-world use, feedback, and iterative design.

An additional concern regarding the application of the pre-certification program to health IT developers is the impact on the viability of any potential false claims act cases. A large deterrent in making false statements to the federal government is the false claims act. However, under a "recognition" program, no false statement as to the capability of a CEHRT is actually made. Thus, as it relates to false statements, cases like eClinicalworks and Greenway would not be viable under the false claims act because no statement was made regarding the capability of a CEHRT. Instead, the business reputation is evaluated. For example, in Greenway, the Department of Justice alleged that Greenway falsely represented to the certifying entity performing the testing and certification that its software met the required certification criteria to obtain certification. If, however, Greenway or any other health IT developer participated in the "recognition" program, it would not make any certification or statement as to whether its products meet the certification requirements.

We recognize that some EHR vendors (e.g., eClinicalWorks, Greenway Health) were accused of falsifying ONC certification, which included product testing. However, we view this as an additional reason why health IT developers, and entities new into the EHR space, should not be provided a less stringent path to certification than is currently available. If anything, ONC should intensify its testing and validation of health IT products.

Request for Information on the Development of Similar Independent Program Processes

Recognition of the FDA Software Pre-Certification Program for purposes of certification of health IT to 2015 Edition criteria may eventually be determined to be infeasible or insufficient to meet our goals of reducing burden and promoting innovation. With this in mind, we request comment on whether ONC should establish new regulatory processes tailored towards recognizing the unique characteristics of health IT (e.g., electronic health record (EHR) software) by looking first at the health IT developer, rather than primarily at the health IT presented for certification, as is currently done under the Program. We also welcome more specific comments on the health IT developer criteria for such an approach and what the Conditions and/or Maintenance of Certification requirements should be to support such an approach within the framework of the proposed Conditions and Maintenance of Certification requirements discussed in section VII of this proposed rule.

Preamble FR Citation: 84 FR 7439 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

Please see the attached comments from the AMA on the FDA's Software Pre-Certification Program.

Section IV – Updates to the 2015 Edition Certification Criteria

§ 170.213 United States Core Data for Interoperability (USCDI)

We propose to adopt the USCDI at new § 170.213: “Standard. United States Core Data for Interoperability (USCDI), Version 1 (v1) (incorporated by reference in § 170.299).”

We propose to revise the following 2015 Edition certification criteria to incorporate the USCDI standard in place of the “Common Clinical Data Set” (currently defined at § 170.102 and proposed for removal in this rule):

- ‘‘Transitions of care’’ (§ 170.315(b)(1));
- ‘‘view, download, and transmit to 3rd party’’ (§ 170.315(e)(1));
- ‘‘consolidated CDA creation performance’’ (§ 170.315(g)(6));
- ‘‘transmission to public health agencies—electronic case reporting’’ (§ 170.315(f)(5)); and
- ‘‘application access—all data request’’ (§ 170.315(g)(9)).]

Preamble FR Citation: 84 FR 7441 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Please see 84 FR 7567-68 for estimates related to this proposal.

Public Comment Field:

The AMA supports ONC’s proposal to require all certified health IT systems to comply with the U.S. Core Data for Interoperability version 1 (USCDI). ONC identifies the USCDI as a standardized set of health data classes and constituent data elements for nationwide, interoperable health information exchange.[1] Currently, the data that is “exposed” by an EHR (e.g., the common clinical data set, or CCDS) is often a subset of what most would consider a complete medical record. Health IT vendors can provide data beyond the required minimum but have historically not gone beyond certification requirements. **Ultimately, all health IT should provide access and use of a patient’s entire longitudinal medical record in a computable format. Usability, however, should not be trumped by quantity.** “Perfect” may be all electronic health information, but “good” is what can practically be accessed, used, or exchanged; we should not let perfect be the enemy of good. Information that is minimally necessary should be structured to provide optimal usability. Not all data needs to be standardized, but it should be computable. **The USCDI provides objective structure with standards that moves us closer to a computable medical record.** We agree with ONC that “the USCDI standard aims to achieve the goals set forth in the Cures Act by specifying a common set of data classes for interoperable exchange”, but much more needs to be done.

The AMA urges ONC to prioritize its effort to establish and follow a predictable, transparent, and collaborative process to expand the USCDI, including providing stakeholders with the opportunity to comment on the USCDI’s expansion. The accelerated addition of data classes and elements—along with additional context around these data (i.e., metadata)—is vital to meeting the goals of Cures. It is also logical to include pricing, cost, and administrative transaction standards in the USCDI version expansion. This will support the Administration’s goal to bolster a health care market economy, facilitate price transparency, and vastly expand the number of ways in which a beneficiary can access and utilize such information. Additionally, coding and terminologies that support a patient’s use of his or her health information will become increasingly vital. Descriptors are available that supports the translation of medical jargon into

[1] U.S. Core Data for Interoperability, 2019 version 1, available at: https://www.healthit.gov/isa/sites/isa/files/inline-files/USCDIv12019revised.pdf

consumer-friendly information. **Immediately following the publication of its final rule, ONC should establish a formal USCDI submission, review, and validation process to ensure clinician perspectives are considered.** As ONC considers the structure and processes necessary to expand the USCDI, the AMA recommends ONC adopt the Health Information Technology Advisory Committee (HITAC) USCDI Task Force's recommendations dated April 18, 2018. This is a critical need to build consensus across the health care system. The AMA is uniquely qualified to support this effort.

The AMA has established an Integrated Health Model Initiative (IHMI) that leverages collaborative communities, a physician-led validation and review process, and advanced data modeling to support improvement in data use and exchange. IHMI is recognized by ONC's Interoperability Proving Ground and by the Health Information Technology Advisory Committee's Interoperability Standards Priorities Task Force. IHMI works with over 30 health care stakeholders, including major technology developers, informaticists, terminologists, consumer groups, professional associations, clinicians, and standards development organizations. **The AMA offers our IHMI to support cross-stakeholder agreement related to data standardization/modeling, medical knowledge representation, and efforts around data portability/liquidity.**

We do not support requiring both health IT developers and users of certified health IT to concurrently develop, test, implement, train, and use EHRs with these updates within a 24-month timeline. Health IT development requires a separate timeline than the adoption and use of products by physicians. We suggest ONC continue to allow CMS to designate the update timeline for CEHRT. ONC should clarify that its proposed timeline does not include the 12+ months needed for physicians and other health care providers to schedule product updates/installations, test deployments, train staff, and safely use new EHRs.

Updated Versions of Vocabulary Standard Code Sets

We propose that the USCDI Version 1 (USCDI v1) include the newest versions of the "minimum standard" code sets included in the CCDS available at publication of a subsequent final rule. We request comment on this proposal and on whether this could result in any interoperability concerns. To note, criteria such as the 2015 Edition "family health history" criterion (§ 170.315(a)(12)), the 2015 Edition "transmission to immunization registries" criterion (§ 170.315(f)(1)), and the 2015 Edition "transmission to public health agencies—syndromic surveillance" criterion (§ 170.315(f)(2)) reference "minimum standard" code sets; however, we are considering changing the certification baseline versions of the code set for these criteria from the versions adopted in the 2015 Edition final rule to ensure complete interoperability alignment. We welcome comment on whether we should adopt such an approach.

Preamble FR Citation: 84 FR 7441 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Not Applicable

Public Comment Field:

The AMA supports the requirement to use the newest version of the "minimum standard" code sets included in the CCDS available at publication of a subsequent final rule for the USCDI. This approach has worked well in previous Edition updates and we anticipate that so long as newer versions maintain a reasonable degree of backward compatibility there should be little concern for ongoing interoperability.

We note that USCDI classes combined with HL7 based specifications (resources, profiles, etc.) and implementation guides for how to "implement" classes in USCDI are a step in the right direction. However, gaps will likely exist in HL7 specifications and implementation guides due to unambiguous, machine interpretable meaning relative to a set of clinically valid data requirements. For example, the latest version of the US Core FHIR profile for blood pressure (BP) would allow multiple disparate groups to create BP measurements with a body site specified in SNOMED CT. These groups are valid relative to the US Core profiles and valid relative to the USCDI. However, they are not computably equivalent based on what is in the FHIR observation instance. This is a core issue that should be addressed to ensure semantic interoperability.

The AMA has established an Integrated Health Model Initiative (IHMI) that leverages collaborative communities, a physician-led validation and review process, and advanced data modeling to support improvement in data use and exchange. IHMI is recognized by ONC's Interoperability Proving Ground and by the Health Information Technology Advisory Committee's Interoperability Standards Priorities Task Force. IHMI works with over 30 health care stakeholders, including major technology developers, informaticists, terminologists, consumer groups, professional associations, clinicians, and standards development organizations. **The AMA offers our IHMI to support cross-stakeholder agreement related to data standardization/modeling, medical knowledge representation, and efforts around data portability/liquidity.**

The AMA's IHMI is prepared to support portability standards for provenance, clinical notes, and other data classes in the USCDI. The IHMI offers its support in leading development of the USCDI and is well-positioned to lead pilots of USCDI v2.X through participation in HITAC, HL7/FHIR Accelerator, and the IHMI community of collaborators. The IHMI could can assist by:

- Creating FHIR profiles that define what should be captured to make the data more clinically valuable and define how to capture the data to improve the semantic consistency of FHIR based data. Doing this leads to less ambiguity so that data from disparate sources is more computationally equivalent and comparable.

- Create software services that help "data makers" ensure the data they are creating is clinically valid to support its intended use and so that "data users" receiving data can interpret the intended meaning consistently and safely. The current state of the art in delivering these kinds of services rely on custom, fit-for-purpose mappings between alternative representations that have the same or similar meanings. Mapping can help bridge the semantic gaps mentioned, but this approach is error prone and finding a way to capture and exchange data more consistently between trading partners and decreasing reliance on mapping-based solutions is a better, more sustainable, and scalable path.

The USCDI v1 includes new data elements for "address" and "phone number." The inclusion of "address" (to represent the postal location for the patient) and "phone number" (to represent the patient's telephone number) would improve the comprehensiveness of health information for patient care. The AMA strongly supports inclusion of these new data classes and data types. We recommend ONC point towards established standards for address, such as the USPS standard.

The USCDI v1 also includes a new data class "provenance." Provenance has been identified by stakeholders as valuable for interoperable exchange. ONC proposes to further delineate the provenance data class into three data elements: "the author," which represents the person(s) who is responsible for the information; "the author's time stamp," which indicates the time the information was recorded; and "the author's organization," which would be the organization the author is associated with at the time they interacted with the data. ONC requests comment on the inclusion of these three data elements and whether any other provenance data elements—such as the identity of the individual or entity the data was obtained from or sent by (sometimes referred to as data's "last hop")—would be essential to include as part of the USCDI v1 standard. The AMA supports this new data class and data elements. However, we anticipate that more granularity will be needed for Provenance Data Elements, such as "role of the individual," (e.g., ordering/verifying/supervisor author) and "patient identification". Patient identification would be useful to include in provenance to track usage and ensure governance and consented use aligns with patient preference. The AMA recommends ONC make "Provenance" a functional requirement, rather than a named standard given that more work needs to be done before an industry consensus standard is available.

As ONC considers the structure and processes necessary to expand the USCDI, the AMA recommends ONC adopt the Health Information Technology Advisory Committee (HITAC) USCDI Task Force's recommendations dated April 18, 2018. These recommendations include:

- Establishing a six-stage maturation process through which data classes would be promoted, each with objective characteristics for promotion;
- Expanding the USCDI as each data class completes stages 1-4 without a predetermined timeline;
- Establishing an annual publishing cycle for the USCDI with periodic bulletins as data objects/data classes progress from one stage to the next;
- Incorporating public feedback in each stage;
- Testing USCDI process by addressing critical trusted exchange framework requirements;
- Ensuring the voice of the patient is represented and heard;
- Supporting the process of data object harmonization as a condition for data class advancement
- Establishing a process for data class management; and
- Establishing a governance structure for the USCDI.

Unique Device Identifier (UDI) for a Patient's Implantable Devices: CDA Implementation Guide

The recently published Health Level 7 (HL7®) CDA R2 Implementation Guide: C-CDA Supplemental Templates for Unique Device Identification (UDI) for Implantable Medical Devices, Release 1-US Realm identifies changes needed to the C-CDA to better facilitate the exchange of the individual UDI components in the health care system when devices are implanted in a patient. We request comment on whether we should add this recently published UDI IG as a requirement for health IT in order to meet the requirements for UDI USCDI Data Class. In addition, we do not have a reliable basis on which to estimate how much it would cost to meet the requirements outlined in the UDI IG; and, therefore, we request comment on the cost and burden of complying with this proposed requirement.

Preamble FR Citation: 84 FR 7443 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Not Applicable

Public Comment Field:

The AMA supports requiring the new UDI IG as a requirement for health IT. The UDI for medical devices aims to improve post-market surveillance and patient safety. While the AMA strongly supports the incorporation of the UDI on medical devices, there is some debate about the most appropriate place to capture this information. CMS and the FDA have called for including part of the UDI in the next claims form template update—slated for 2021. However, certification requirements allow EHRs to capture and transmit the full UDI. The AMA views EHRs and registries as the most appropriate method to capture and manage the UDI. We do not support capturing UDI information in administrative claims as it represents a significant cost to providers, as well as the industry, and claims information does not follow a patient as they switch insurers. The claims form changes would also not require the capture of the full UDI, instead capturing only the device identifier ("DI") portion and excluding the product identifier portion. Both the Production Identifier and DI are key in providing the complete picture about a medical device when safety issues arise. Capturing this information in a patient's EHR allows the full medical device information to follow patients, and their longitudinal medical history, regardless of changes in insurance.

§ 170.205(a) Patient summary record

We propose to adopt the HL7 CDA® R2 Implementation Guide: C-CDA Templates for Clinical Notes R1 Companion Guide, Release 1 C-CDA Companion Guide to support best practice implementation of USCDI v1 data classes and enhance the implementation of other 2015 Edition certification criteria that also reference Consolidated Clinical Document Architecture (C-CDA) Release 2.1 (§ 170.205(a)(4)). Those criteria include:

- "transitions of care" (§ 170.315(b)(1));
- "clinical information reconciliation and incorporation" (§ 170.315(b)(2));
- "care plan" (§ 170.315(b)(9));
- "view, download, and transmit to 3rd party" (§ 170.315(e)(1));
- "consolidated CDA creation performance" (§ 170.315(g)(6)); and
- "application access – all data request" (§ 170.315(g)(9)).

Preamble FR Citation: 84 FR 7443 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

The AMA supports the adoption of the HL7 CDA® R2 Implementation Guide: C-CDA Templates for Clinical Notes R1 Companion Guide, Release 1 C-CDA Companion Guide. We seek clarity from ONC on its plan to include sufficient testing for this release.

§ 170.205(b) Electronic prescribing

* * *

(1) Standard. National Council for Prescription Drug Programs (NCPDP), Script Standard Implementation Guide, Version 2017071 (incorporated by reference in § 170.299).

Preamble FR Citation: 84 FR 7444 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

The AMA supports aligning the certification criteria to the SCRIPT 2017071, as CMS has retired SCRIPT 10.6 and adopted 2017071 effective January 2020 for Part D. We recognize there may be challenges and expenses for practices to upgrade with their EHR vendor, but given the fact that the new version of SCRIPT will be required under Medicare Part D, it would seem helpful to have the EHR certification criteria in alignment to require the same version of SCRIPT. It is our understanding is that SCRIPT 2017071 is not backwards compatible with SCRIPT 10.6, which is why—unlike with previous electronic prescribing (eRx) standard updates—these is no transition period. We agree with permitting continued certification to 10.6 if the eRx criteria are finalized prior to January 2020 makes sense in this regard. However, we seek clarity on timing. Would this mean a physician could purchase and upgrade to a 2017071 EHR before January 2020, but not "flip the switch" to implement until January 1st?

We suggest that, along with certifying the rest of the SCRIPT 2017071 transactions required by CMS, ONC should require certification to the SCRIPT electronic prior authorization (ePA) transactions included in the 2017071 standard. We are aware that lack of vendor support for the ePA transactions is a major barrier to physician use of the transactions—only 21 percent of physicians in our PA survey reported that their EHR supports prescription ePA.

SCRIPT 2017071 includes the new RxTransferRequest, RxTransferResponse, and RxTransferConfirm transactions which allow for one pharmacy to request the transfer of a prescription from another pharmacy. These transactions allow the transfer of unfilled controlled substance prescriptions—including Schedule II—between pharmacies. Facilitating interpharmacy transfer would be useful for all stakeholders involved.

ONC discusses collaborating with the Centers for Disease Control and Prevention (CDC) on a project to translate the CDC's Guideline for Prescribing Opioids for Chronic Pain into FHIR Clinical Decision Support (CDS) Hooks in EHRs, noting that "not all states have adopted the guideline, not all physicians are aware of them, and sound opioid prescribing guidelines are far from universally followed." **It is critical that physicians be allowed to override the CDS Hooks if the patient's unique clinical situation warrants departure from the guideline.** These guidelines are already being treated like one-size-fits-all mandate. HHS' Interagency Pain Care Task Force has highlighted growing inability of CDC guidelines to appropriately individualize patient care. The AMA has also sent a letter to HHS addressing our concerns with misapplied CDC guidelines. We do not support CDS Hooks preventing the physician from prescribing medically necessary, appropriate opioid treatment.

The AMA has concerns with the federal government nationalizing prescription drug monitoring program (PDMP) requirements. States have demonstrated they can make independent decisions on PDMP and improving the workflow and EHR integration. We encourage states to implement and modernize PDMPs that are seamlessly integrated into the physician’s normal workflow, and provide clinically relevant, reliable information at the point of care. This helps physicians and other health care professionals better understand a patient’s full prescription history to make more informed clinical decisions. A modernized PDMP, moreover, means that states should share access to PDMP data across state lines, within the safeguards applicable to protected health information as well developing uniform data standards to facilitate the sharing of information across state lines.

AMA research has shown significant uptake in the use of PDMPs. From 2014 to 2017, PDMP registration increased from approximately 471,000 registrants to more than 1.5 million authorized users of a PDMP. Use also greatly increased from 61.5 million queries in 2014 to more than 300 million in 2017. The AMA attributes this increase in use mainly to the improved functionality of PDMPs, although we acknowledge that certain state mandates contribute to the increased use. Preliminary review of 2018 data show that PDMP use continues to increase.

The AMA also acknowledges that PDMP growth is likely due, in part, to improvements in technology and state policy that support interstate interoperability. States have spent considerable resources in both areas. There is no question that this has been greatly enhanced by the work of the National Association of Boards of Pharmacy (NABP) InterConnect Platform, which has connected more than 45 states as well as the Defense Health Agency. These connections, moreover, are underpinned with memorandums of understanding and other agreements between states on many issues, including how a state will respect and follow the patient privacy laws of partnering states.

The AMA has concerns that the CDC “Overdose Data to Action” Notice of Funding Opportunity and FY2018 Comprehensive Opioid Abuse Site-based Program Category 5 Department of Justice (DOJ) grants could adversely affect state PDMPs and the physicians and other health care professionals who use them to help inform their clinical decision making. We note that ONC does not specifically discuss this issue; however, we believe federal agencies involved in PDMP policy should be aware of potential unintended consequences.

The AMA considers the information in a PDMP to be protected health information due the highest level of patient privacy protections. While we have concerns that some state laws do not offer the strongest safeguards possible, this is an evolving area in state policy that must not be put in potential jeopardy by requiring states to use new privacy and other standards as required by the CDC and DOJ, which may have even fewer privacy safeguards. It is also unclear how a new data sharing system could impact the improvements in state PDMPs to share information between states. Given that the current system appears to be working in terms of interstate interoperability, the AMA is concerned that a new mandate could interrupt and adversely affect what is currently working.

§ 170.315(c)(3) Clinical quality measures – report

Included in 2015 Edition Base EHR Definition? *No*

Clinical quality measures – report. Enable a user to electronically create a data file for transmission of clinical quality measurement data in accordance with the implementation specifications specified in § 170.205(h)(3) and (k)(3).

Preamble FR Citation: 84 FR 7446 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

The AMA supports that health IT be certified to the criterion that supports CMS QRDA Implementation Guidleines (IGs). The AMA has long advocated for CMS and ONC to align electronic clinical quality measure (eCQM) certification with one standard rather than requiring EHRs to certify to HL7's quality reporting document architecture (QRDA) IG when most EHRs must also support CMS' "form and manner" IG. Requiring consolidated clinical document architecture (C-CDA), QRDA, and CMS' form and manner conformance was excessive for vendors and variations in CMS' IGs meant that information had to be modeled differently for reporting and direct patient care. However, we recommend that ONC monitor this part of the certification process for unintended consequences since CMS' IGs are updated on a yearly basis and CERHT only occurs every few years. Given the lack of alignment with timing, eCQM measures and standards will continue to lack testing.

To reduce burden, ONC should consider a certification approach that permits vendors to only certify to standards based on the care setting(s) they serve. If a vendor serves both in-patient and outpatient settings, then they should have to certify to both settings to meet the various demands and needs of the providers.

§ 170.315(b)(10) Electronic health information export

Included in 2015 Edition Base EHR Definition? *Yes*

Electronic health information export.

(i) Single patient electronic health information export.

(A) Enable a user to timely create an export file(s) with all of a single patient's electronic health information the health IT produces and electronically manages on that patient.

(B) A user must be able to execute this capability at any time the user chooses and without subsequent developer assistance to operate.

(C) Limit the ability of users who can create such export file(s) in at least one of these two ways:

(1) To a specific set of identified users.

(2) As a system administrative function.

(D) The export file(s) created must be electronic and in a computable format.

(E) The export file(s) format, including its structure and syntax, must be included with the exported file(s).

(ii) Database export. Create an export of all the electronic health information the health IT produces and electronically manages.

(A) The export created must be electronic and in a computable format.

(B) The export's format, including its structure and syntax must be included with the export.

(iii) Documentation. The export format(s) used to support single patient electronic health information export as specified in paragraph (b)(10)(i) of this section and database export as specified in paragraph (b)(10)(ii) of this section must be made available via a publicly accessible hyperlink.

Preamble FR Citation: 84 FR 7446-49 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Please see 84 FR 7568-70 for estimates related to this proposal.

Public Comment Field:

The AMA strongly supports patients' right to have access to complete copies of their entire medical record in a computable format. We see the spirit of this new criterion as aligned with this right, but we caution that the electronic health information (EHI) Export for Patient Access needs refinement as proposed.

There are several layers of ambiguity that will inhibit uniform implementation and widespread use of this functionality. First, we note that patients requesting an EHI export will likely obtain vastly different payloads based on three factors: (1) the health IT developers certified to deliver the export; (2) the implementation decisions and customizations at each implementation; and (3) the institution's interpretation of what constitutes EHI. Second, we note that widespread use of this functionality will be inhibited because the task of making sense of the data falls largely on patients and families, not the developers or clinicians delivering the export.

Export difference across developers
Given that ONC does not propose specific transport, content, or syntax standards for EHI export (either Patient Access or Database Export), it is difficult to understand how ONC will judge conformance to this criterion. As we have seen in numerous other certification criteria, it is likely that developers are much more uniform in their conformance testing than in the real world, and it is very likely that this lack of specificity will deliver different exports for similar patients.

Export differences based on implementation decisions and customizations
ONC expects that EHI exports will encompass "all the EHI that the health IT system produces and electronically manages for a patient or group of patients." Holding aside the ambiguity of "produces and electronically manages," there is the simple fact that health care facilities have made implementation decisions and customizations that likely differ across sites, even when using the same developer, which will enable some systems to deliver data that other systems cannot.

Export differences based on interpretation of EHI definition
ONC defines EHI broadly. Generally, physicians have struggled to define the Designated Record Set (DRS) consistently, which by comparison is a more constrained concept. Given that the definition of EHI does not dictate which data must be delivered via Patient Access and Database Export, there is a high probability that institutional interpretations will create difference in what similar patients receive as part of this criterion.

The AMA recommends ONC look for ways to constrain and/or guide implementation of these policies, while keeping the intent of these policies broad and inclusive. Specifically, the AMA recommends ONC:

- **Constrain EHI Export to comport with HIPAA's electronic protected health information (ePHI) regulation;**
- **Specify that transport standard for EHI Export for Patient Access leverage RESTful protocols; and**
- **Include EHI Export for Patient Access (§ 170.315 (b)(10)(i)) among the requisite criteria of real world testing plans, proposed elsewhere in this NPRM.**

By specifying a functional, yet non-exclusive, set of standards for EHI (i.e., ePHI) to be made available via API, we anticipate that industry stakeholders and government regulators can work toward a standardized API for managing export requests in future rulemakings, even as the non-USCDI data payloads themselves are likely to remain developer-specific (i.e. non-standardized) for some time into the future. Further, this paradigm will encourage more innovation to make the data useful to patients and families than a single and/or periodic "data dump" as the current proposal portends.

The EHI Export for Patient Access should be tied to "HIPAA compliant uses," which would be physician access for treatment, payment, or operations for the purposes of continuity of care, and patient data access for whatever purpose they deem appropriate. We stress that until such time EHR vendors utilize an API orchestration to provide patients direct EHI export capabilities, the ability to request an EHI export be medical practice-facing. We have concerns with the potential of hundreds or thousands of users' "requests" coming into an EHR for an export. This would severely bog down an EHR's performance, putting patients at risk. Furthermore, externally-facing EHI export capabilities (i.e., download or export functions provided via patient portals), would expose an EHR to denial-of-service attacks (DoS). To be clear, patients could still request their ePHI from the medical practice, but the act of querying the EHR should be reserved for authorized users, administrators, and medical office staff. Until such time that EHR vendors have proven capable of supporting patient-facing EHI requests while also mitigating privacy and security issues, EHI Export should be protected from potential abuse or exploitation.

We do not support inclusion of "software programs or services," as a "user" in the context of EHI Export for Patient Access without express consent from the patient, the patient's legal guardian, or caregiver. Given the current regulatory gaps that exist outside HIPAA, we are concerned that health app terms and conditions could expose all of a patients EHI without the patient's knowledge or desire. In addition, ONC needs to provide clear guidance and education.

Transitions Between Health IT Systems aka Database Export
ONC proposes that a health IT developer of health IT certified to this criterion must, at a customer's request, provide a complete export of all EHI that is produced or managed by means of the developer's certified health IT.

The AMA strongly supports this functionality to require EHR vendors to follow protocols during EHR data transitions to reduce common barriers that prevent physicians from changing EHR vendors including high costs, time, and risk of losing patient data.

We also generally support the flexibility regarding how the outcome of a database export is achieved so long as the system provides the relevant data dictionary and documentation, as outlined by ONC, <u>and is required to complete a Database Export as part of initial Certification and consume a Database Export as part of initial Certification.</u> Alternatively, a certified developer could demonstrate its capacity to deliver and consume a Database Export as part of real world testing Maintenance of Certification requirements. To meet the spirit of this criterion a certified developer should be able to perform an export relatively easily and a different certified developer should be able to consume the export equally easily.

We recommend that imaging reports, at a minimum, be among the image elements shared as part of the EHI Export. If a specific medical-grade image is requested by the patient, physicians may not have processes to deliver this information to the patient. Many physicians can only link to images in picture archiving and communication systems (PACS)—even if this is through their EHR. These images can be many hundreds or thousands of megabytes in size.

ONC should require health IT developers to publish as part of the export format documentation the types of EHI they cannot support for export. Without this documentation, determining what has been done will simply be impossible and over time, never determinable.

Continuity care documents (CCDs) contain critical patient information that is structured and coded (unlike the EHI proposal). The structured/coded contents of CCDs are important for automated migration of patient data when physician organizations switch from one EHR to another. Hence, we recommend that that 2015 Edition certification requirement be retained at least until the new EHI Export functionality is implemented and in use and we understand the degree of structuring/coding and standardization that EHR vendors will implement in complying with the new EHI proposal.

AMA appreciates ONC's proposal that for provider-mediated requests, a developer may design the health IT to limit the type of users that would be able to access and initiate EHI export functions. To further address potential privacy and security concerns, ONC may want to consider adding "authenticated" to the regulatory language involving the user in proposed § 170.315(10)(i). Specifically, in subparagraph (A) "Enable a<u>n authenticated</u> user to timely create an export file(s) . . ." and in subparagraph (B) "A<u>n authenticated</u> user must be able to execute . . .". This authentication can help ensure that the individual health care professional or his or her office staff are authorized to access a patient's medical record for proper export. The authentication does not need to be stringent or administratively burdensome and could be as simple as a user name and password when logging into an EHR.

§ 170.315(d)(12) Encrypt authentication credentials

Included in 2015 Edition Base EHR Definition? *No*

Encrypt authentication credentials. Health IT developers must assess their Health IT Modules' capabilities and make one of the following attestations:

(i) "Yes." Health IT Module encrypts stored authentication credentials in accordance with standards adopted in § 170.210(a)(2).

(ii) "No." Health IT Module does not encrypt stored authentication credentials.

Preamble FR Citation: 84 FR 7450 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Please see 84 FR 7575 for estimates related to this proposal.

Public Comment Field:

The AMA supports this proposal.

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

Included in 2015 Edition Base EHR Definition? *No*

Multi-factor authentication. Health IT developers must assess their Health IT Modules' capabilities and make one of the following attestations:

(i) "Yes." Health IT Module supports authentication through multiple elements the identity of the user with industry recognized standards.

(ii) "No." Health IT Module does not support authentication through multiple elements the identity of the user with industry recognized standards.

Preamble FR Citation: 84 FR 7450-51 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Please see 84 FR 7575 for estimates related to this proposal.

Public Comment Field:

The AMA generally supports this proposal.

However, the AMA highlights the barriers to implement multi-factor authentication for the electronic prescription of controlled substances (EPCS). As the AMA described in a March 2018 letter to the Drug Enforcement Administration (DEA), the current EPCS regulations, which have been unchanged since 2010, prevent user-friendly devices that are widely available in medical practices from being deployed to meet the multifactor authentication standards in the DEA rules. Current regulations have also driven down EPCS adoption. The AMA letter outlined specific changes needed in the regulations for biometric devices to improve and reduce physician burden. These requests are consistent with a recommendation from the President's Commission on Combating Drug Addiction and the Opioid Crisis.

We stress that ONC should not stipulate multi-factor requirements on EHRs and continue to only seek "yes" / "no" attestation. Prior to recommending or proposing any multi-factor requirements (i.e., standards, processes, or functions) for EHRs, ONC should coordinate with the DEA through the lens of reducing physician burden—with focus on cost, usability, interoperability, and effectiveness of EPCS system regulation.

§ 170.315(b)(12) Data segmentation for privacy – send

Included in 2015 Edition Base EHR Definition? *No*

Data segmentation for privacy – send. Enable a user to create a summary record formatted in accordance with the standard adopted in § 170.205(a)(4) and (a)(4)(i) that is tagged as restricted at the document, section, and entry (data element) level and subject to restrictions on re-disclosure according to the standard adopted in § 170.205(o)(1).

Preamble FR Citation: 84 FR 7452 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Please see 84 FR 7575-77 for estimates related to this proposal.

Public Comment Field:

The AMA supports this proposal.

§ 170.315(b)(13) Data segmentation for privacy – receive

Included in 2015 Edition Base EHR Definition? *No*

Data segmentation for privacy – receive. Enable a user to:

(i) Receive a summary record that is formatted in accordance with the standard adopted in § 170.205(a)(4) and (a)(4)(i) that is tagged as restricted at the document, section, and entry (data element) level and subject to restrictions on re-disclosure according to the standard adopted in § 170.205(o)(1); and

(ii) Preserve privacy markings to ensure fidelity to the tagging based on consent and with respect to sharing and re-disclosure restrictions.

Preamble FR Citation: 84 FR 7452 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Please see 84 FR 7575-77 for estimates related to this proposal.

Public Comment Field:

The AMA supports this proposal.

§ 170.315(g)(11) Consent management for APIs

Included in 2015 Edition Base EHR Definition? *No*

Consent management for APIs.

(i) Respond to requests for data in accordance with:

(A) The standard adopted in § 170.215(c)(1); and

(B) The implementation specification adopted in § 170.215(c)(2).

(ii) Documentation.

(A) The API(s) must include complete accompanying documentation that contains, at a minimum:

(1) API syntax, function names, required and optional parameters supported and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns.

(2) The software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s).

(3) All applicable technical requirements and attributes necessary for an application to be registered with an authorization server.

(B) The documentation used to meet paragraph (g)(11)(ii)(A) of this section must be available via a publicly accessible hyperlink.

Preamble FR Citation: 84 FR 7453 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Please see 84 FR 7575 for estimates related to this proposal.

Public Comment Field:

Existing standards such as Consent2Share (C2S) and Data Segmentation for Privacy (DS4P) are not being utilized due to cost, maturity, or lack of adoption. We appreciate that ONC is proposing C2S and DS4P as optional certification criteria for health IT and that the DS4P proposal requires segmentation at the element level (as opposed to the document level). We understand that DS4P is viewed as a major development challenge for EHR vendors. In discussing privacy with the Substance Abuse and Mental Health Services Administration (SAMHSA), we have learned that FHIR-enabled C2S APIs provide both physician and patient-facing services and the infrastructure to segment data and manage consent. **We support requiring C2S in Base EHR health IT certification and encourage ONC to increase C2S adoption.** We are also aware that there is no longer funding to continue this important work. **The AMA recommends ONC coordinate with SAMHSA to establish a public-private project to advance C2S.** Vendors and payers have expressed the need to address "the dual challenges of data standardization and easy information access" with the goal "to help payers and providers to positively impact clinical, quality, cost and care management outcomes."[2] We expect health IT vendors and payers would welcome a public-private C2S effort. We recommend an analogous process to that of the Da Vinci Project, but one that is open, transparent, and excludes membership fees. The USCDI and the Interoperability Standards Advisory should be leveraged for support.

[2] Health Level 7, Da Vinci Project, available at: http://www.hl7.org/about/davinci/

Note: Because this template presents comment tables in the order in which the new and revised provisions of 45 CFR parts 170 and 171 are discussed in the preamble of the proposed rule, comment tables for other new and revised certification criteria, standards, and definitions can be found in Section VII, below.

§ 170.523 Principles of proper conduct for ONC-ACBs (Authorized Certification Bodies)

* * * * *

(a) Accreditation. Maintain its accreditation in good standing to ISO/IEC 17065 (incorporated by reference in § 170.599).

* * * * *

(f) Reporting. * * *

~~(2)~~ [Reserved]

(g) Records retention.

(1) Retain all records related to the certification of Complete EHRs and Health IT Modules to an edition of certification criteria beginning with the codification of an edition of certification criteria in the Code of Federal Regulations through a minimum of 3 years from the effective date that removes the applicable edition from the Code of Federal Regulations; and

(2) Make the records available to HHS upon request during the retention period described in paragraph (g)(1) of this section;

(h) Testing. Only certify Health IT Modules that have been:

(1) Tested, using test tools and test procedures approved by the National Coordinator, by an:

(i) ONC-ATL;

(ii) ONC-ATL, NVLAP-accredited testing laboratory under the ONC Health IT Certification Program, and/or an ONC-ATCB for the purposes of performing gap certification; or

(2) Evaluated by it for compliance with a conformance method approved by the National Coordinator.

* * * * *

(k) Disclosures. * * *

(1) All adaptations of certified Health IT Modules;

(2) All updates made to certified Health IT Modules affecting the capabilities in certification criteria to which the “safety-enhanced design” criteria apply;

(3) All updates made to certified Health IT Modules in compliance with § 170.405(b)(3) and (4); and;

(4) All voluntary standards updates successfully made to certified Health IT Modules per § 170.405(b)(5).

* * * * *

(p) Real world testing.

(1) Review and confirm that applicable health IT developers submit real world testing plans in accordance with § 170.405(b)(1).

(2) Review and confirm that applicable health IT developers submit real world testing results in accordance with § 170.405(b)(2).

§ 170.523 Principles of proper conduct for ONC-ACBs (Authorized Certification Bodies)

(3) Submit real world testing plans by December 15 of each calendar year and results by April 1 of each calendar year to ONC for public availability.

(q) Attestations. Review and submit health IT developer Conditions and Maintenance of Certification attestations made in accordance with § 170.406 to ONC for public availability.

(r) Test results from ONC-ATLs. Accept test results from any ONC-ATL that is:

(1) In good standing under the ONC Health IT Certification Program, and

(2) Compliant with its ISO 17025 accreditation requirements.

(s) Information for direct review. Report to ONC, no later than a week after becoming aware of, any information that could inform whether ONC should exercise direct review under § 170.580(a).

(t) Standards Voluntary Advancement Process Module Updates Notices. Ensure health IT developers opting to take advantage of the Standards Version Advancement Process flexibility per § 170.405(b)(5) provide timely advance written notice to the ONC-ACB and all affected customers.

(1) Maintain a record of the date of issuance and the content of developers' § 170.405(b)(5) notices; and

(2) Timely post content of each § 170.405(b)(5) notice received publicly on the CHPL attributed to the certified Health IT Module(s) to which it applies.

Preamble FR Citation: 84 FR 7456-57 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Please see 84 FR 7559 and 84 FR 7582-84 for estimates related to this proposal.

Public Comment Field:

The AMA seeks clarity from ONC as to what metrics the National Coordinator will use to approve a conformance method. We are especially interested in ONC's plan to ameliorate fraudulent certification practices (e.g., eClinicalWorks, Greenway Health) given these proposals.

The AMA supports ONC's proposal to include a detailed description of all known material information concerning additional types of costs or fees that a user may be required to pay to implement or use the Health IT Module's capabilities—whether to meet provisions of HHS programs requiring the use of certified health IT or to achieve any other use within the scope of the health IT's certification.

Approach to Health IT for the Care Continuum and the Health Care of Children

Section 4001(b)(i) of the Cures Act instructs the National Coordinator to encourage, keep, or recognize, through existing authorities, the voluntary certification of health IT under the Program for use in medical specialties and sites of service for which no such technology is available or where more technological advancement or integration is needed. This provision of the Cures Act closely aligns with ONC's ongoing collaborative efforts with both federal partners and stakeholders within the health care and health IT community to encourage and support the advancement of health IT for a wide range of clinical settings. Section VI of this proposed rule outlines our approach to implement Section 4001(b) of the Cures Act, which requires that the Secretary make recommendations for the voluntary certification of health IT for use by pediatric health providers and to adopt certification criteria to support the voluntary certification of health IT for use by pediatric health providers to support the health care of children. To be clear, and consistent with past practice, we do not recommend or propose a "pediatric-specific track or program" under the ONC Health IT Certification Program. This proposed rule outlines the certification criteria adopted in the 2015 Edition which we believe support the certification of health IT for pediatric care.

Preamble FR Citation: 84 FR 7457-61 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Not applicable

Public Comment Field

Congress has recognized that EHRs designed for use in adult populations may overlook differences when caring for children and introduce the opportunity for medical errors. For example, unlike adults, children often receive medication doses based on their weight.

These errors can occur, in part, due to poor system usability—which refers to how the layout, customization, configuration, and implementation of EHRs affects their use by clinicians. Inadequate usability has two major consequences. First, ineffective usability can contribute to clinician burden and burnout, which can make them more susceptible to making errors. Second, poor usability can contribute directly to patient harm through errors that occur when clinicians interact with the EHR.

Research, published in *Health Affairs* last year, revealed that EHR usability contributed to medication errors in 3,243 of 9,000 safety events examined. Of those usability-related events, more than 80 percent involved an inappropriate drug dose, and 609 of the usability-related events reached patients. In one case, a transplant patient missed days-worth of medication that would help prevent organ rejection. In another case, the blood transfusion for a newborn in critical condition was delayed due to the inability to create a record. These findings, including other research conducted by MedStar Health, indicate a clear link between the usability of EHRs and patient safety.

The new pediatric-focused criteria required by Cures provides ONC with an opportunity to improve usability and the safety of EHRs used to care for children.

To implement that provision in Cures, ONC identified 10 clinical priorities for pediatric care extracted in large part from the Children's Electronic Health Record Format—a resource developed by the Agency for Healthcare Research and Quality to assist with the design of EHRs.

These priorities include functions that are distinct or common in pediatric care, such as weight-based drug dosing, using biometric norms to monitor growth, and age- and weight-specific single-dose medication range checking. In the proposed rule, ONC rightly identified those areas where additional pediatric focus in EHR design could improve care. ONC selected provisions in its existing and newly proposed criteria that can support these clinical priorities, and developed worksheets to demonstrate how they would apply to pediatric care.

ONC can further enhance its proposed criteria both in the overall implementation of the program and by further mapping other aspects of certification to pediatric care.

Overall recommendations to enhance the program

ONC should consider the following recommendations to improve the overall program for EHRs used in the care of children.

- *Require All Use Cases*: ONC should clarify that only those technologies that meet all the required criteria can obtain the pediatric-focused certification. Otherwise, technologies may receive certification for some of the clinical priorities, and health care facilities may inadvertently believe that the system supports all 10 clinical priorities.

- *Develop Specific Guidance*: ONC should further develop specific and detailed guidance or implementation specifications for each proposed pediatric clinical priority to assist EHR developers and testing organizations in assessing conformance with the pediatric clinical priorities. ONC has developed this type of guidance for certification in the past (e.g., the Certification Companion Guide).

- *Use Pediatric and Usability Expertise*: ONC should involve pediatric and usability experts in the development of implementation guides and test procedures for the pediatric clinical priorities. For example, ONC should involve pediatricians, pediatric nurses, and human factors experts in developing those resources.

- USCDI expansion: ONC should consider expanding the USCDI v1 to include “gestational age at birth” and “Obstetrics History”. The impact of gestational age on pediatric health outcomes later in childhood is well documented, and we believe making this valuable information readily available to physicians would lead to improved patient care.

The AMA supports the Health IT for the Care Continuum Task Force Recommendations for voluntary certification of health IT for pediatric care. We are particularly supportive of Recommendation 8: Associate maternal health information and demographics with newborn. Linking maternal and neonatal health information is a vital step in implementing meaningful value-based maternity care models. Current methods for linking these data are complex, burdensome, and unreliable. As a result, most value-based maternity care models are unable to associate neonatal outcomes with prenatal care, and therefore cannot fully appreciate the impact of this care on health care costs or outcomes.

We recommend that ONC consult women’s health physicians to ensure that the appropriate data elements are included for the care of adolescent women and girls.

The AMA agrees with ONC that the proposal to support a more granular approach to data segmentation and consent management would be applicable to women’s health providers who wish to limit the sharing of a minor’s reproductive and sexual health EHI. It would also allow physicians to segment information about child abuse and other sensitive situations to protect children and adolescents. In the event that maternal health information is linked to her neonate’s, data segmentation will also be required if the mother does not remain the child’s legal guardian throughout their childhood. We urge ONC to ensure that granular data segmentation technology is affordable and accessible to all providers, including pediatric and women’s health physicians. We strongly believe that, as EHI is shared more freely, the capability to segment data will become increasingly important.

Additional opportunities to map the criteria to pediatric care

In the proposed rule, ONC aligns the technical worksheets for each of the 10 clinical priorities with certification criteria from ONC's 2015 edition and changes made to the criteria through these regulations. ONC should extend that approach—mapping criteria from existing requirements—to other aspects of the pediatric-focused criteria in several ways.

- *Specify use of pediatric-focused test scenario:* Under current regulations, EHR developers must use testing scenarios to show that they comply with ONC's 2015 edition certification requirements. For the pediatric-focused certification, ONC should clarify that some of the testing scenarios used be EHR developers should involve pediatric patients and pediatric-specific factors.

- *Include pediatric end-users*: As part of those testing scenarios, EHR developers must involve at least 10 end users to conduct the assessments under current regulations. As the proposed rule is currently drafted pediatric end-users are not necessarily required to be involved in the testing of a product for pediatric-focused certification. Recognizing the unique aspects of pediatric care, ONC should require the involvement of pediatric-focused clinicians—such as pediatricians and pediatric nurses—among the 10 required for end-user testing for those technologies that are also obtaining pediatric-focused certification For pediatric-focused certification, at least five of all the end-users testing a product should be clinicians who care for pediatric patients to obtain robust input from end users with experience caring for children. Recognizing that some EHR developers may not have access to additional end-users for testing, the pediatric clinicians could be included within the minimum 10 end-user requirement, and not as an additional requirement.

- *Require use of simulated pediatric patient data*: EHR developers use data on simulated patients to demonstrate that their technologies meet ONC's certification program. ONC supplies some test data for those assessments. For a pediatric-focused certification, ONC should supply test data for simulated pediatric patients and clarify that the test data used must involve simulated data of children.

Request for Information on Health IT and Opioid Use Disorder Prevention and Treatment

We seek comment in this proposed rule on a series of questions related to health IT functionalities and standards to support the effective prevention and treatment of opioid use disorder (OUD) across patient populations and care settings. Specifically, we request public comment on how our existing Program requirements (including the 2015 Edition certification criteria) and the proposals in this rulemaking may support use cases related to OUD prevention and treatment and if there are additional areas that ONC should consider for effective implementation of health IT to help address OUD prevention and treatment. This section also includes request for comment on furthering adoption and use of electronic prescribing of controlled substances standard and neonatal abstinence syndrome.

Preamble FR Citation: 84 FR 7461-65 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

The AMA recommends focusing attention on improving the integration of prescription drug monitoring programs (PDMPs) with EHRs and to facilitate electronic prescribing of controlled substances (EPCS). Additional burden reduction can be accomplished through adoption of the PDMP recommendations included on page 17 of the HHS Interagency Pain Management Best Practices Task Force draft report:

- Recommendation 1b calls for clinicians to be trained on accessing and interpreting PDMP data, and 1c says physicians should engage patients to discuss their PDMP data rather than making a judgement that may result in the patient not receiving appropriate care.
- Regarding burden reduction specifically, Recommendation 1d states the health care provider team should determine when to use PDMP data, and that PDMP use should not be mandated without proper clinical indications to avoid unnecessary burden in the inpatient setting.
- Recommendation 1e calls for studies to identify where PDMP data are best used, with PDMP use adjusted based on the study findings to minimize undue burdens and overutilization of resources.
- Recommendation 1f calls for EHR vendors to work to integrate PDMPs in their system design at minimal to no additional cost to providers.

The AMA encourages ONC to consider the Pain Management Task Force recommendations as it develops OUD regulation.

The AMA also highlights the current barriers EPCS. As the AMA described in a March 2018 letter to the Drug Enforcement Administration (DEA), the current EPCS regulations, which have been unchanged since 2010, prevent user-friendly devices that are widely available in medical practices from being deployed to meet the multifactor authentication standards in the DEA rules. Current regulations have also driven down EPCS adoption. The AMA letter outlined specific changes needed in the regulations for biometric devices to improve and reduce physician burden. These requests are consistent with a recommendation from the President's Commission on Combating Drug Addiction and the Opioid Crisis that the DEA should increase EPCS uptake to prevent diversion and forgery and revise the EPCS regulations. We appreciate HHS' recognition of Section 2003(c) of the Substance Use–Disorder Prevention that Promotes Opioid Recovery and Treatment for Patients and Communities Act (P.L. 115-271), which calls on the Attorney General/DEA to "update the requirements for the biometric component of multifactor authentication with respect to electronic prescriptions of controlled substances." Current regulations are impeding the implementation of EPCS. Removing these barriers will significantly reduce fraudulent prescriptions for opioid analgesics and increase the adoption of EPCS to combat the epidemic of opioid overdose deaths. ONC should coordinate with the DEA through the lens of reducing physician burden—with particular focus on cost, usability, interoperability, and effectiveness of EPCS system regulation.

Section VII – Conditions and Maintenance of Certification

Note: Because this template presents comment tables in the order in which their subject proposed provisions are discussed in the preamble of the proposed rule, this section includes tables for certain new and revised provisions in 45 CFR subparts A, B, C, and E, in complement to the proposed new subpart D.

§ 170.401 Information blocking Condition and Maintenance of Certification Requirement
(a) Condition of Certification. A health IT developer must not take any action that constitutes information blocking as defined in 42 U.S.C. 300jj-52 and § 171.103. (b) Maintenance of Certification. [Reserved]
Preamble FR Citation: 84 FR 7465 **Specific questions in preamble?** *No*
Regulatory Impact Analysis: Not applicable
Public Comment Field: The AMA supports this requirement. Physicians participating in the Quality Payment Program are already required to attest to a three-part information blocking statement. This statement is detailed and ties a physician's attestation to their EHR vendor's capabilities. For instance, physicians must attest they "implemented in a manner that allowed for the timely, secure, and trusted bidirectional exchange of structured electronic health information with other health care providers (as defined by 42 U.S.C. 300jj(3)), including unaffiliated providers, and with disparate CEHRT and health information technology (HIT) vendors." This is clearly technical and outside the control of most physicians. Alignment of expectations and requirements across stakeholders is necessary to ensure information blocking is curtailed. HHS should also strive for consistent policies to limit confusion. The AMA recommends ONC require CEHRT attest to the same three requirements physicians are held accountable to.

§ 170.402 Assurances

(a) Condition of Certification.

(1) A health IT developer must provide assurances satisfactory to the Secretary that the health IT developer will not take any action that constitutes information blocking as defined in 42 U.S.C. 300jj-52 and § 171.103, unless for legitimate purposes specified by the Secretary; or any other action that may inhibit the appropriate exchange, access, and use of electronic health information.

(2) A health IT developer must ensure that its health IT certified under the ONC Health IT Certification Program conforms to the full scope of the certification criteria.

(3) A health IT developer must not take any action that could interfere with a user's ability to access or use certified capabilities for any purpose within the scope of the technology's certification.

(4) A health IT developer that manages electronic health information must certify health IT to the certification criterion in § 170.315(b)(10).

(b) Maintenance of Certification.

(1) A health IT developer must retain all records and information necessary to demonstrate initial and ongoing compliance with the requirements of the ONC Health IT Certification Program for:

(i) A period of 10 years beginning from the date each of a developer's health IT is first certified under the Program; or

(ii) If for a shorter period of time, a period of 3 years from the effective date that removes all of the certification criteria to which the developer's health IT is certified from the Code of Federal Regulations.

(2) A health IT developer that must comply with the requirements of paragraph (a)(4) of this section must provide all of its customers of certified health IT with the health IT certified to the certification criterion in § 170.315(b)(10) within 24 months of this final rule's effective date or within 12 months of certification for a health IT developer that never previously certified health IT to the 2015 Edition, whichever is longer.

Preamble FR Citation: 84 FR 7465-66 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Please see 84 FR 7577-78 for estimates related to this proposal.

Public Comment Field:

The AMA generally supports these requirements.

ONC is proposing several changes to its certification program, including § 170.315(g)(10)-APIs, EHI export, USCDI adoption, Real World Testing, Standards Version Advancement Process, Communications, and Assurances. The AMA appreciates ONC responding to our advocacy on these issues. As previously stated, EHR vendors will require a considerable amount of time to make changes and comply with Conditions and Maintenance of Certification. 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 final rule's effective date. Because most physicians 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 physician EHR adoption, implementation, and use concurrently.** Not only does this create an incredibly ambitious timeline, it also effectively usurps CMS' authority to determine when physicians use a particular Edition of Certified EHR Technology (CEHRT) requirements for incentive program participation.

EHR developers should be provided a specific timeline to develop, test, certify, publish, implement, and train their customers on new product features and functions. This timeline should be separate from physician adoption requirements, which is squarely in CMS' purview. While we support a two-year time horizon for development, implementation, and go-live, we do not support ONC dictating the adoption schedule for physicians. If ONC continues with its proposal it should, at the very least, provide physicians additional time beyond 24 months. Once our members have entered into their vendor's implementation queue, they continue to experience 12+ month timelines before EHRs are upgraded/installed. We reiterate that ONC should remain focused on the technology, while other HHS agencies and offices dictate adoption policies. We also caution ONC against using language that implies that both certified health IT developers and their customers are required to meet the 24-month timeline (e.g., health IT developers "must provide all of its customers…"); this wording extends ONC's regulatory reach beyond health IT developers to providers. Rather, ONC should require that health IT developers "make available" to its customers upgraded product features and functions within 24 months.

For this reason and to prevent significant confusion for physicians about program requirements, the AMA strongly recommends ONC refrain from adjusting the 2015 Edition Base EHR definition. We do not agree with ONC's reasoning to not propose 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 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.

Trusted Exchange Framework and the Common Agreement – Request for Information

We request comment as to whether certain health IT developers should be required to participate in the Trusted Exchange Framework and Common Agreement (TEFCA) as a means of providing assurances to their customers and ONC that they are not taking actions that constitute information blocking or any other action that may inhibit the appropriate exchange, access, and use of EHI. We also welcome comment on the certification criteria we have identified as the basis for health IT developer participation in the Trusted Exchange Framework and adherence to the Common Agreement, other certification criteria that would serve as a basis for health IT developer participation in the Trusted Exchange Framework and adherence to the Common Agreement, and whether the current structure of the Trusted Exchange Framework and Common Agreement are conducive to health IT developer participation and in what manner.

Preamble FR Citation: 84 FR 7466-67 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

Overall, the AMA supports the general goals of trusted exchange networks (TEN), including the ability to (1) provide physicians access to health information about their patients, regardless of where the patient received care; (2) provide patients and their caregivers to access their health information electronically without special effort; and (3) ensure that organizations accountable for managing benefits and the health of populations can receive necessary and appropriate information on a group of individuals.

We encourage ONC to address issues of physician choice and voluntary participation when evaluating the use of TENs to facilitate interoperability. We note that some of the potential use cases outlined in ONC's draft TEF raised questions as to physicians' ability to willingly participate (or not participate) in trust networks. Due to the sensitive nature of electronic health information and the potential disruption to physician practices involved in implementing the required technology, **the AMA underscores the importance of ensuring that physicians understand and can willingly elect to participate in information sharing via TENs. This must be included in any policy related to the TEFCA.**

For instance, in many states and cities, physicians' financial viability is entirely dependent on participation in particular health insurer networks. For example, 43 percent of US metropolitan areas have a single health insurer with at least half of the commercial insurance market share.[3] In locations such as these, physicians would face potentially insurmountable financial disadvantages if they were to choose not to participate in the dominant insurer's network. In turn, this would force physicians to agree to the dominant insurer's terms of participation for a TEN that they might otherwise oppose, including participation in a TEN about which they have technological or security concerns.

Additionally, payers might require a physician to participate in a particular health information exchange network as a condition of participation in a plan. Physicians could also be forced to join multiple TENs based on different health plans' requirements for network providers, resulting in the physician needing to comply with multiple network requirements, policies, and fees. This would likely impose significant burdens upon practices—particularly smaller practices with already strained resources. **As a result, we recommend that ONC include language in its final rule that protects physicians' ability to voluntarily**

[3] American Medical Association, *Metro areas increasingly dominated by single insurance companies* (Oct. 23, 2017), available at https://www.ama-assn.org/press-center/press-releases/metro-areas-increasingly-dominated-single-insurance-companies

join a TEN and prevents insurers (or other entities) from requiring TEN participation as a term of network contracts.

§ 170.403 Communications

(a) Condition of Certification.

(1) A health IT developer may not prohibit or restrict the communication regarding—

(i) The usability of its health IT;

(ii) The interoperability of its health IT;

(iii) The security of its health IT;

(iv) Relevant information regarding users' experiences when using its health IT;

(v) The business practices of developers of health IT related to exchanging electronic health information; and

(vi) The manner in which a user of the health IT has used such technology.

(2) A health IT developer must not engage in any practice that prohibits or restricts a communication regarding the subject matters enumerated in paragraph (a)(1) of this section, unless the practice is specifically permitted by this paragraph and complies with all applicable requirements of this paragraph.

(i) Unqualified protection for certain communications. A health IT developer must not prohibit or restrict any person or entity from communicating any information or materials whatsoever (including proprietary information, confidential information, and intellectual property) when the communication is about one or more of the subject matters enumerated in paragraph (a)(1) of this section and is made for any of the following purposes—

§ 170.403 Communications

~~(A)~~ Making a disclosure required by law;

~~(B)~~ Communicating information about adverse events, hazards, and other unsafe conditions to government agencies, health care accreditation organizations, and patient safety organizations;

~~(C)~~ Communicating information about cybersecurity threats and incidents to government agencies;

~~(D)~~ Communicating information about information blocking and other unlawful practices to government agencies; or

~~(E)~~ Communicating information about a health IT developer's failure to comply with a Condition of Certification, or with any other requirement of this part, to ONC or an ONC-ACB.

(ii) Permitted prohibitions and restrictions. For communications about one or more of the subject matters enumerated in paragraph (a)(1) of this section that is not entitled to unqualified protection under paragraph (a)(2)(i) of this section, a health IT developer may prohibit or restrict communications only as expressly permitted by paragraphs (a)(2)(ii)(A) through (F) of this section.

~~(A)~~ Developer employees and contractors. A health IT developer may prohibit or restrict the communications of the developer's employees or contractors.

(B) Non-user-facing aspects of health IT. A health IT developer may prohibit or restrict communications that disclose information about non-user-facing aspects of the developer's health IT.

~~(C)~~ Intellectual property. A health IT developer may prohibit or restrict communications that would infringe the intellectual property rights existing in the developer's health IT (including third-party rights), provided that—

(1) A health IT developer does not prohibit or restrict, or purport to prohibit or restrict, communications that would be a fair use of a copyright work; and

(2) A health IT developer does not prohibit the communication of screenshots of the developer's health IT, subject to the limited restrictions described in paragraph (a)(2)(ii)(D) of this section.

~~(D)~~ Screenshots. A health IT developer may require persons who communicate screenshots to—

(1) Not alter screenshots, except to annotate the screenshot, resize it, or to redact the screenshot in accordance with § 170.403(a)(2)(ii)(D)(3) or to conceal protected health information;

(2) Not infringe the intellectual property rights of any third parties, provided that—

(i) The developer has used all reasonable endeavors to secure a license (including the right to sublicense) in respect to the use of the third-party rights by communicators for purposes of the communications protected by this Condition of Certification;

(ii) The developer does not prohibit or restrict, or purport to prohibit or restrict, communications that would be a fair use of a copyright work;

(iii) The developer has put all potential communicators on sufficient written notice of each aspect of its screen display that contains third-party content that cannot be communicated because the reproduction would infringe the third-party's intellectual property rights; and

(iv) Communicators are permitted to communicate screenshots that have been redacted to not disclose third-party content; and

§ 170.403 Communications

(3) Redact protected health information, unless the individual has provided all necessary consents or authorizations or the communicator is otherwise authorized, permitted, or required by law to disclose the protected health information.

(E) Pre-market testing and development. A health IT developer may prohibit or restrict communications that disclose information or knowledge solely acquired in the course of participating in pre-market product development and testing activities carried out for the benefit of the developer or for the joint benefit of the developer and communicator. A developer must not, once the subject health IT is released or marketed for purposes other than product development and testing, and subject to the permitted prohibitions and restrictions described in paragraph (a)(2)(ii) of this section, prohibit or restrict communications about matters enumerated in paragraph (a)(1) of this section.

(b) Maintenance of Certification.

(1) Notice. Health IT developers must issue a written notice to all customers and those with which it has agreements containing provisions that contravene paragraph (a) of this section:

(i) Within six months of the effective date of the final rule that any communication or contract provision that contravenes paragraph (a) of this section will not be enforced by the health IT developer.

(ii) Within one year of the final rule, and annually thereafter until paragraph (b)(2)(ii) of this section is fulfilled, that any communication or contract provision that contravenes paragraph (a) of this section will not be enforced by the health IT developer.

(2) Contracts and agreements.

(i) A health IT developer must not establish or enforce any contract or agreement that contravenes paragraph (a) of this section.

(ii) If a health IT developer has a contract or agreement in existence at the time of the effective date of this final rule that contravenes paragraph (a) of this section, then the developer must in a reasonable period of time, but not later than two years from the effective date of this rule, amend the contract or agreement to remove or void the contractual provision that contravenes paragraph (a) of this section.

Preamble FR Citation: 84 FR 7467-76 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Please see 84 FR 7578 for estimates related to this proposal.

Public Comment Field:

The AMA generally supports these requirements with the following recommendations:

(v) The business practices of developers of health IT related to exchanging electronic health information;

In addition to health information exchange, the ONC should explicitly permit communication regarding CEHRT product safety, fees, or other costs associated with product use or maintenance.

(A) Developer employees and contractors. A health IT developer may prohibit or restrict the communications of the developer's employees or contractors.

ONC should clarify that physicians participating in developer programs that test products in real-world environments, or those that volunteer to test products on an ad hoc basis, are not considered developer contractors and therefore should not be restricted from communicating concerns. ONC should further clarify users should not be restricted from communicating concerns about issues unrelated to functions/features they are involved in testing even if they are considered contractors. Communication restrictions should only apply to specific EHR functions/features a "contractor" is directly involved in developing or testing.

(B) Non-user-facing aspects of health IT. A health IT developer may prohibit or restrict communications that disclose information about non-user-facing aspects of the developer's health IT.

ONC should clarify that user-developed examples or diagrams (e.g., flowcharts) are not prohibited. Flowcharts are important tools used in presentations to visually depict complex interfaces and systems. They are often important components in academic and peer-reviewed research.

(i) Within six months of the effective date of the final rule that any communication or contract provision that contravenes paragraph (a) of this section will not be enforced by the health IT developer.

The AMA believes that one month, rather than six months, is sufficient time for health IT developers to contact their clients about current contract provisions. Further delaying physicians' ability to communicate concerns with EHR safety, security, and interoperability could jeopardize patient care. We request ONC explicitly state that any permitted communication made following the effective date of the final rule be inadmissible as a violation of a contract/agreement regardless of whether the customer has been notified.

VII.B.4 Application Programming Interfaces

§ 170.215(a)(2) API Resource Collection in Health

Implementation specifications. API Resource Collection in Health (ARCH) Version 1.

Preamble FR Citation: 84 FR 7479-80 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Please see 84 FR 7570-75 for estimates related to our proposals regarding APIs.

Public Comment Field:

The AMA supports ONC establishment of the proposed API Resource Collection in Health (ARCH). Although we believe that, in general, health IT standards should be developed by standards development organizations (SDOs), we recognize the considerations that lead ONC to publish the ARCH. We ask ONC to emphasize that the ARCH is bounded by the scope of the USCDI, that the USCDI will only include data classes and data elements that have SDO-developed implementation guides, that the ARCH will only reference HL7 FHIR resources, and, moving forward, is transitioned as rapidly as possible to a private sector, SDO-developed implementation specification, such as the HL7 US Core.

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

Included in 2015 Edition Base EHR Definition? *Yes*

Standardized API for patient and population services. The following technical outcomes and conditions must be met through the demonstration of application programming interface technology.

(i) Data response. Respond to requests for data (based on an ID or other token) for each of the resources referenced by the standard adopted in § 170.215(a)(1) and implementation specifications adopted in § 170.215(a)(2) and (3).

(ii) Search support. Respond to search requests for data consistent with the search criteria included in the implementation specification adopted in § 170.215(a)(4).

(iii) App registration. Enable an application to register with the technology's "authorization server."

(iv) Secure connection. Establish a secure and trusted connection with an application that requests data in accordance with the standard adopted in § 170.215(a)(5).

(v) Authentication and app authorization – 1st time connection. The first time an application connects to request data the technology:

(A) Authentication. Demonstrates that user authentication occurs during the process of authorizing the application to access FHIR resources in accordance with the standard adopted in § 170.215(b).

(B) App authorization. Demonstrates that a user can authorize applications to access a single patient's data as well as multiple patients data in accordance with the implementation specification adopted in § 170.215(a)(5) and issue a refresh token that is valid for a period of at least 3 months.

(vi) Authentication and app authorization – Subsequent connections. Demonstrates that an application can access a single patient's data as well as multiple patients data in accordance with the implementation specification adopted in § 170.215(a)(5) without requiring re-authorization and re-authentication when a valid refresh token is supplied and issue a new refresh token for new period no shorter than 3 months.

(vii) Documentation.

(A) The API(s) must include complete accompanying documentation that contains, at a minimum:

(1) API syntax, function names, required and optional parameters supported and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns.

(2) The software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s).

(3) All applicable technical requirements and attributes necessary for an application to be registered with an authorization server.

(B) The documentation used to meet paragraph (g)(10)(vii)(A) of this section must be available via a publicly accessible hyperlink.

Preamble FR Citation: 84 FR 7481-84

Specific questions in preamble? *Yes*

Regulatory Impact Analysis: Please see 84 FR 7570-75 for estimates related to our proposals regarding APIs.

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

Public Comment Field:

The AMA encourages ONC to finalize Option 4: **Adopt only FHIR Release 4 in the final rule.** Release 4 is a normative standard and represents an achievable target for certified health IT in the near-term. While we note that Option 4 places more responsibility on IGs to be up-to-date, we are concerned that previous Releases contain too much optionality. Given our support for FHIR R4, the AMA does not support adoption of associated FHIR Release 2 Implementation Specifications. Rather, we recommend ONC proceed with naming HL7 US Core Implementation Guides. We are cognizant that there is less experience with US Core IGs than Argonaut IGs, yet we anticipate the industry will coalesce around US Core IGs over the coming months—especially if ONC signals FHIR R4 as the standard underpinning the USCDI.

We are concerned ONC's proposal will require physicians to outsource identity management functions. Currently, if a physician trusts an actor—someone they routinely do business with and know well—that physician has an established comfort level with providing access to their health IT system. In this instance, when a patient requests access to their data the physician has a strong level of assurance about the actor. However, ONC is now proposing physicians trust foreign entities to provide identity management. We agree that patients must be able to get data in a simple manner, however if a physician cannot validate software—let alone validate security—then the health care system and patients are exposed to unnecessary risks. We seek clarity from ONC if this is its intent.

Validating the scope of access to patient data via a third-party app presents challenges. Granting access to third parties involves obtaining a token from an app developer then granting access based on the developer's token matching the patient's. However, under ONC's proposal, physicians will lack the ability to routinely audit or validate the scope of authority granted by patients to third-party app developers. ONC suggests this is necessary to reduce friction for patients using apps. We recognize the Office of Civil Rights (OCR) recently released guidance on app use. **However, data privacy should not solely be the responsibility of the patient.** Our members are concerned with the impact on patient-physician relationship if their data are misused. For example, patients will delay or forgo care if they lack trust in a physician's ability to protect their health data. Furthermore, patients cannot reliable expect consumer-facing apps to limit transmission of their data to other third-party entities. ONC's policy requires physicians and patients take the word of the developer on data use and reuse. We seek clarity from ONC if this is its intent.

In addition to constraining ONC's information blocking regulations and interpretation of EHI, ONC should require that all certified APIs include mechanisms to strengthen patients' control over their data. The AMA has heard concerns from consumer groups and patient advocates about the volume, variety, and velocity of data that will be shared without assurances of privacy and security. We again reiterate that patients should have complete access to their data. HIPAA reinforces this right. The AMA believes that patients are just as interested in protecting their data's privacy as they are in accessing it. As previously discussed, the complex set of regulatory unknows may encourage oversharing or unfettered access and use. Indeed, many companies are well-positioned to benefit from this.

In reading the proposals, we also question the level of deference provided to entities seeking to commoditize patient data. Information that is collected has been likened to a "digital tattoo" that is impossible to expunge.[4] The Equifax hack in 2017 exposed nearly 148 million individuals' information.[5] Equifax is considered by many as a regular credit reporting agency. However, its activities as a data broker generate significant profit.[6] The data "buying and selling" ecosystem is increasingly intertwined—making it more likely the patient information will be *traded* not just exchanged. For example, recent reports note the ability of even innocuous-seeming gaming apps to glean and monetize revealing user data:

> *The intricacies of gameplay data can tell you a lot about what makes people tick, and what's going on with them — studies have shown that you play games differently when you're depressed, or dieting. "Nobody gets too upset about games," Nieborg says. "But the underlying technology is really powerful. These people are really pushing the technology to the limits where the potential for abuse is massive."*
>
> *"There's a massive incentive to know a lot about your players," he says, and the "dark twist" is that "If you can do this for a games company and you're really good at it, you can [then go] start working for other companies that have less trivial goals than just selling digital gems to people."*[7]

The data leak is not limited to gaming information. Apps, particularly free apps, often use advertisements to generate revenue. The advertisements collect and share an individual's advertising ID—a string of numbers and letters that identify an individual and keep a log of his or her clicks, searches, purchases, and sometimes geographic location as he or she moves through various apps.[8] While the information is often deemed anonymous, the information can be "shockingly easy to de-anonymize, and that hundreds of apps collect 'anonymous' real-time location data that needs only the slimmest additional context clues to tie to an individual person."[9] **If ONC prioritizes making patients the center of their care, and states that patient access to data on their smartphones will enable this, what is ONC doing to ensure that patients do not become products?**

We also note that Draft 2 of the Trusted Exchange Framework and Common Agreement (TEFCA) specifically raises concerns with non-HIPAA entities' use of electronic health information.

> Individuals, health care providers, health plans, and networks may not be willing to exchange data through the Common Agreement if smartphone app developers and other non-HIPAA entities present privacy or security risks because they are not obligated to abide by the HIPAA Rules. In order to meet the goals of the Cures Act as well as to help address these concerns and encourage robust data exchange that will ultimately improve the health of patients, the Common Agreement requires non-HIPAA entities, who elect to participate in exchange, to be bound by certain provisions that align with safeguards of the HIPAA Rules. This will bolster data integrity, confidentiality, and security, which is necessary given the evolving cybersecurity threat landscape.[10]

[4] The New York Times, *We're Not Going to Take It Anymore*, April 2019, available at: https://www.nytimes.com/2019/04/10/opinion/internet-privacy-regulation.html#click=https://t.co/XvdMfPlIBv

[5] Money, *The Equifax Hack Affects 143 Million People. Here's What Makes It Even Worse*, September 2017, available at: http://money.com/money/4933204/equifax-hack-credit-report-identity-theft/?iid=sr-link7

[6] Fast Company, *Here are the data brokers quietly buying and selling your personal information*, March 2019, available at: https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information

[7] Vox Media Network, *Angry Birds and the end of privacy*, May 2019, available at: https://www.vox.com/explainers/2019/5/7/18273355/angry-birds-phone-games-data-collection-candy-crush

[8] Id.

[9] Id.

[10] ONC, *Trusted Exchange Framework and Common Agreement (TEFCA) Draft 2*, 2019, available at: https://www.healthit.gov/sites/default/files/page/2019-04/FINALTEFCAQTF41719508version.pdf

We are confused by the dichotomy between ONC's proposed rule and the clear concern outlined in the TEFCA. ONC should ensure its multiple proposals and regulations are aligned with patient privacy and app developer requirements.

If patients access their health data—some of which could contain family history and could be sensitive—through a smartphone, they must have a clear understanding of the potential uses of that data by app developers. Most patients will not be aware of who has access to their medical information, how and why they received it, and how it is being used (for example, an app may collect or use information for its own purposes, such as an insurer using health information to limit/exclude coverage for certain services, or may sell information to clients such as to an employer or a landlord). The downstream consequences of data being used in this way may ultimately erode a patient's privacy and willingness to disclose information to his or her physician. ONC's proposal requires API usage without requiring that the API technology include privacy controls. **The technological capability to implement privacy controls exists, so by failing to implement them, the agency is making a deliberate policy decision to not prioritize privacy.**

To assist in resolving this issue, the AMA has identified an opportunity for multiple coexisting components to empower patients with meaningful knowledge and control over the use of their data. We believe that ONC has the responsibility to provide patients with a basic level of privacy and app transparency—especially since some apps deliberately hide their actions and make it difficult for patients to learn about or control their data. The AMA urges ONC to take the following steps to ensure patient data are accessed, exchanged, and used pursuant with the goals outlined in Cures and the desires expressed by patients.

As part of an API Technology Supplier's certification, **ONC should require APIs check an app's attestation to:**

- **Industry-recognized development guidance;**
- **Transparency statements and best practices; and**
- **The adoption of a model notice to patients.**

One possible method to accommodate this would require an EHR vendor's API to check for three "yes/no" attestations from any consumer-facing app. For example, 1) An app developer could choose to assert conformance to Xcertia's Privacy Guidelines.[11] 2) An app developer could attest to the Federal Trade Commission's (FTC) Mobile Health App Developers: FTC Best Practices and the CARIN Alliance Code of Conduct. 3) An app developer could attest to adopting and implementing ONC's Model Privacy Notice. These could be viewed as value-add services as proposed by ONC. The app could be acknowledged or listed by the health IT developer in some special manner (e.g., in an "app store," "verified app" list). We would urge EHR vendors to also publicize the app developers' attestations; ONC could also require a vendor to do so as a prerequisite to product certification.

We do not believe that requiring an API check for an app developer attestation would be a significant burden on API Technology Suppliers. We recognize that a "yes" attestation would not ensure apps implement or conform to their attestations. However, we firmly believe this will provide a needed level of assurance to patients and would be greatly welcomed by users. **We also believe this could act as a "bookend"—placing app developers between ONC health IT certification requirements (which would be imposed by API Technology Suppliers), and FTC's enforcement of unfair and deceptive practices. In other words, an app developer would be strongly motivated to attests "yes" and to act in line with their attentions.**

[11] Both the Food and Drug Administration (FDA) and ONC participate on the board of Xcertia, a multi-stakeholder effort to develop guidelines and recommendations for medical app development.

We are aware there are some who believe requiring this minimum level of privacy controls for patients is "paternalistic." This characterization is perplexing given that patient privacy is a fundamental aspect of Cures, necessary for patients to safeguard themselves from data profiteering and discrimination, and promoted by the AMA Code of Medical Ethics and House of Delegates, which includes representation from state and territorial medical associations, national medical specialty organizations, and the federal government. As noted above, one of the purposes of Cures is to provide individuals with access to their health information without special effort. Most consumers would probably characterize multiple pages' worth of privacy practices, which may or may not be transparent, as requiring special effort. So why does the agency charged with implementing Cures dismiss concern over patient privacy with a "buyer beware" mentality? It is alarming that ONC appears to view its charge as merely providing access to data, and not meaningfully empowering the patient as the spirit of Cures intended.

The AMA recommends ONC work with OCR and other responsible agencies to provide formal guidance on current uses of FHIR APIs, such as in SMART on FHIR applications or CDS Hooks services, with respect to compliance with relevant privacy and security regulations, such as HIPAA (e.g., the inappropriate sending of full patient demographic details, the inappropriate use of broadly-scoped data access tokens).

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

The following Condition of Certification applies to developers of Health IT Modules certified to any of the certification criteria adopted in § 170.315(g)(7) through (11).

(a) Condition of Certification.

(1) General. An API Technology Supplier must publish APIs and must allow health information from such technology to be accessed, exchanged, and used without special effort through the use of APIs or successor technology or standards, as provided for under applicable law, including providing access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws.

(2) Transparency conditions.

(i) General. The business and technical documentation published by an API Technology Supplier must be complete. All documentation published pursuant to paragraph (a)(2)(ii) of this section must be published via a publicly accessible hyperlink that allows any person to directly access the information without any preconditions or additional steps.

(ii) Terms and conditions.

(A) Material information. The API Technology Supplier must publish all terms and conditions for its API technology, including any fees, restrictions, limitations, obligations, registration process requirements, or other similar requirements that would be needed to:

~~(1)~~ Develop software applications to interact with the API technology;

~~(2)~~ Distribute, deploy, and enable the use of software applications in production environments that use the API technology;

~~(3)~~ Use software applications, including to access, exchange, and use electronic health information by means of the API technology;

~~(4)~~ Use any electronic health information obtained by means of the API technology; and

~~(5)~~ Register software applications.

(B) API fees. Any and all fees charged by an API Technology Supplier for the use of its API technology must be described in detailed, plain language. The description of the fees must include all material information, including but not limited to:

(1) The persons or classes of persons to whom the fee applies;

(2) The circumstances in which the fee applies; and

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

~~(3)~~ The amount of the fee, which for variable fees must include the specific variable(s) and methodology(ies) that will be used to calculate the fee.

(C) Application developer verification. An API Technology Supplier is permitted to institute a process to verify the authenticity of application developers so long as such process is objective and the same for all application developers and completed within 5 business days of receipt of an application developer's request to register their software application for use with the API Technology Supplier's API technology.

(3) Permitted fees conditions.

(i) General conditions.

(A) All fees related to API technology not otherwise permitted by this section are prohibited from being imposed by an API Technology Supplier.

(B) For all permitted fees, an API Technology Supplier must:

~~(1)~~ Ensure that fees are based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests.

~~(2)~~ Ensure that fees imposed on API Data Providers are reasonably related to the API Technology Supplier's costs of supplying and, if applicable, supporting API technology to, or at the request of, the API Data Provider to whom the fee is charged.

~~(3)~~ Ensure that the costs of supplying and, if applicable, supporting the API technology upon which the fee is based are reasonably allocated among all customers to whom the API technology is supplied, or for whom the API technology is supported.

~~(4)~~ Ensure that fees are not based in any part on whether the requestor or other person is a competitor, potential competitor, or will be using the API technology in a way that facilitates competition with the API Technology Supplier.

(ii) Permitted fee – Development, deployment, and upgrades. An API Technology Supplier is permitted to charge fees to an API Data Provider to recover the costs reasonably incurred by the API Technology Supplier to develop, deploy, and upgrade API technology for the API Data Provider.

(iii) Permitted fee – Supporting API uses for purposes other than patient access. An API Technology Supplier is permitted to charge fees to an API Data Provider to recover the incremental costs reasonably incurred by the API Technology Supplier to support the use of API technology deployed by or on behalf of the API Data Provider. This permitted fee does not include:

(A) Any costs incurred by the API Technology Supplier to support uses of the API technology that facilitate a patient's ability to access, exchange, or use their electronic health information;

(B) Costs associated with intangible assets (including depreciation or loss of value), except the actual development or acquisition costs of such assets; or

(C) Opportunity costs, except for the reasonable forward-looking cost of capital.

(iv) Permitted fee – Value-added services. An API Technology Supplier is permitted to charge fees to an API User for value-added services supplied in connection with software that can interact with the API technology, provided that such services are not necessary to efficiently and effectively develop and deploy such software.

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

(v) Record-keeping requirements. An API Technology Supplier must keep for inspection detailed records of any fees charged with respect to the API technology, the methodology(ies) used to calculate such fees, and the specific costs to which such fees are attributed.

(4) Openness and pro-competitive conditions. General condition. An API Technology Supplier must grant an API Data Provider the sole authority and autonomy to permit API Users to interact with the API technology deployed by the API Data Provider.

(i) Non-discrimination.

(A) An API Technology Suppler must provide API technology to API Data Providers on terms that are no less favorable than it provides to itself and its own customers, suppliers, partners, and other persons with whom it has a business relationship.

(B) The terms on which an API Technology Supplier provides API technology must be based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests.

(C) An API Technology Supplier must not offer different terms or service on the basis of:

(1) Whether the API User with whom an API Data Provider has a relationship is a competitor, potential competitor, or will be using electronic health information obtained via the API technology in a way that facilitates competition with the API Technology Supplier.

(2) The revenue or other value the API User with whom an API Data Provider has a relationship may derive from access, exchange, or use of electronic health information obtained by means of API technology.

(ii) Rights to access and use API technology.

(A) An API Technology Supplier must have and, upon request, must grant to API Data Providers and their API Users all rights that may be reasonably necessary to access and use API technology in a production environment, including:

(1) For the purposes of developing products or services that are designed to be interoperable with the API Technology Supplier's health information technology or with health information technology under the API Technology Supplier's control;

(2) Any marketing, offering, and distribution of interoperable products and services to potential customers and users that would be needed for the API technology to be used in a production environment; and

(3) Enabling the use of the interoperable products or services in production environments, including accessing and enabling the exchange and use of electronic health information.

(B) An API Technology Supplier must not condition any of the rights described in paragraph (a)(4)(ii)(A) of this section on the requirement that the recipient of the rights do, or agree to do, any of the following:

(1) Pay a fee to license such rights, including but not limited to a license fee, royalty, or revenue-sharing arrangement.

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

(2) Not compete with the API Technology Supplier in any product, service, or market.

(3) Deal exclusively with the API Technology Supplier in any product, service, or market.

(4) Obtain additional licenses, products, or services that are not related to or can be unbundled from the API technology.

(5) License, grant, assign, or transfer any intellectual property to the API Technology Supplier.

(6) Meet additional developer or product certification requirements.

(7) Provide the API Technology Supplier or its technology with reciprocal access to application data.

(iii) Service and support obligations. An API Technology Supplier must provide all support and other services reasonably necessary to enable the effective development, deployment, and use of API technology by API Data Providers and their API Users in production environments.

(A) Changes and updates to API technology. An API Technology Supplier must make reasonable efforts to maintain the compatibility of its API technology and to otherwise avoid disrupting the use of API technology in production environments.

(B) Changes to terms and conditions. Except as exigent circumstances require, prior to making changes or updates to its API technology or to the terms and conditions thereof, an API Technology Supplier must provide notice and a reasonable opportunity for its API Data Provider customers and registered application developers to update their applications to preserve compatibility with API technology and to comply with applicable terms and conditions.

(b) Maintenance of Certification.

(1) Registration for production use. An API Technology Supplier with health IT certified to the certification criterion adopted in § 170.315(g)(10) must register and enable all applications for production use within 1 business day of completing its verification of an application developer's authenticity, pursuant to paragraph (a)(2)(ii)(C) of this section.

(2) Service Base URL publication. API Technology Supplier must support the publication of Service Base URLs for all of its customers, regardless of those that are centrally managed by the API Technology Supplier or locally deployed by an API Data Provider, and make such information publicly available (in a computable format) at no charge.

(3) Rollout of (g)(10)-Certified APIs. An API Technology Supplier with API technology previously certified to the certification criterion in § 170.315(g)(8) must provide all API Data Providers with such API technology deployed with API technology certified to the certification criterion in § 170.315(g)(10) within 24 months of this final rule's effective date.

Preamble FR Citation: 84 FR 7485-95 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Please see 84 FR 7570-75 for estimates related to this proposal.

Public Comment Field:

The AMA recommends ONC clarify what is considered an acceptable relationship between the API Technology Supplier and the API User, or clarify what activities are expected or permitted to occur between the API Technology Suppliers and API Users. There are multiple relationships supported in this environment and this relationship is not sufficiently addressed in the proposed rule preamble.

The AMA recommends ONC clarify the requirements and expectations around the app registration condition of certification. We request clarification on following:

- What the practice of "registration" consists of, does not consist of, and who is responsible for keeping a list of registered apps.
- What "verifying the identity" of an API user consists of, does not consist of, and who is responsible for performing this. As previously mentioned, physicians do not have the training or capability to accommodate this. Physicians should be excused from possible cases where API Users misrepresent themselves.
- What "vetting" an app (in contrast to verifying identity of a user) consists of, what falls outside the definition of vetting, who is responsible for vetting, and who is prohibited from vetting. As previously mentioned, physicians do not have the training or capability to accommodate this. Physicians should be excused from possible cases where apps misrepresent themselves.

The AMA has concerns with the concept of "Dynamic Registration". Specifically, we have concerns with ONC's statement that the "verification process would need to focus specifically on the application developer—not its software application(s)". As discussed in our comments on ONC's proposals to leverage the FDA's Pre-Certification Program, verifying an app at the developer level is insufficient to ensure app performance. This concern is compounded when app developers have no previous record of creating safe and effective products in the health care space.

The AMA has identified an opportunity for multiple coexisting components to empower patients with meaningful knowledge and control over the use of their data. We believe that ONC has the responsibility to provide patients with a basic level of privacy and app transparency—especially since some apps deliberately hide their actions and make it difficult for patients to learn about or control their data. The AMA urges ONC to take the following steps to ensure patient data are accessed, exchanged, and used pursuant with the goals outlined in Cures and the desires expressed by patients.

As part of an API Technology Supplier's certification, **ONC should require APIs check an app's attestation to:**

- **Industry-recognized development guidance;**
- **Transparency statements and best practices; and**
- **The adoption of a model notice to patients.**

One possible method to accommodate this would require an EHR vendor's API to check for three "yes/no" attestations from any consumer-facing app. For example, 1) An app developer could choose to assert conformance to Xcertia's Privacy Guidelines. [12] 2) An app developer could attest to the Federal Trade Commission's (FTC) Mobile Health App Developers: FTC Best Practices and the CARIN Alliance Code of Conduct. 3) An app developer could attest to adopting and implementing ONC's Model Privacy Notice. These could be viewed as value-add services as proposed by ONC. The app could be acknowledged or listed by the health IT developer in some special manner (e.g., in an "app store," "verified app" list). We would urge EHR vendors to also publicize the app developers' attestations; ONC could also require a vendor to do so as a prerequisite to product certification.

[12] Both the Food and Drug Administration (FDA) and ONC participate on the board of Xcertia, a multi-stakeholder effort to develop guidelines and recommendations for medical app development.

We do not believe that requiring an API check for an app developer attestation would be a significant burden on API Technology Suppliers. We recognize that a "yes" attestation would not ensure apps implement or conform to their attestations. However, we firmly believe this will provide a needed level of assurance to patients and would be greatly welcomed by users. **We also believe this could act as a "bookend"—placing app developers between ONC health IT certification requirements (which would be imposed by API Technology Suppliers), and FTC's enforcement of unfair and deceptive practices. In other words, an app developer would be strongly motivated to attests "yes" <u>and</u> to act in line with their attentions.**

The AMA appreciates ONC's efforts to address excessive fees charged by EHR vendors to connect their products with other health IT systems, health information exchanges, and third-party applications. We recognize that API permitted fees and restrictions is a multi-pronged issue. Developing policy to accommodate every interaction between an API Technology Supplier, API Data Provider, and API User is untenable. While ONC has attempted to address most scenarios, the resulting proposed fee policy is complex and has limited usefulness for physicians. Our members are already expressing concerns over the increased costs they will encounter to hire consultants or seek legal support just to parse out the rights and responsibilities of each API actor. We are concerned the proposed fee structure will ultimately designate physicians as the default revenue stream for EHR vendors and app developers.

The AMA believes a more practical approach would be to establish a tiered fee structure for APIs. For instance, ONC could establish categories where the technology requirements designate the fees.

- A "no fee" category would limit API Technology Suppliers from charging API Data Providers or API Users any fees for exchanging data in compliance with federal requirements (e.g., costs associated with health information exchange, patient access, reporting quality measures, and data segmentation for privacy). Since all API Technology Suppliers will be certified by ONC, any API Technology Supplier-to-API Technology Supplier connections would also be in the "no fee" category.
- An "at cost" category would allow API Technology Suppliers to charge API Data Providers or API Users the cost of interfacing APIs with a non-API Technology Supplier's commercial technology (e.g., commercial lab systems, commercial picture archiving and communication systems (PACS), commercial data analytics services).
- A "cost plus reasonable profit" category would allow API Technology Suppliers to charge API Data Providers or API Users a reasonable profit when conducting legitimate custom API development or creating custom apps (e.g., creating proprietary mappings for technology unique to a health system or establishing connections with non-commercially available technology.)

For the "at cost" and "cost plus reasonable profit" categories, API Technology Suppliers should be restricted from implementing health IT in non-standard ways that unnecessarily increase the costs, complexity, and other burden of accessing, exchanging, or using EHI. We do not expect all scenarios will be addressed by this approach; however, we believe a clearer and more approachable fee structure will better empower physicians to be informed consumers of technology. We believe this also establishes fair and equitable fee structure for all parties involved.

The AMA seeks clarification on how to reconcile (1) an API Data Provider having "sole authority" to permit API Users to interact with API technology with (2) a patient being able to access their EHI via any API-enabled application they choose without special effort. If a patient accesses their EHI through any app of their choice, how does an API Data Provider, such as a physician, have sole authority to permit API users, such as a patient, to interact with specific API technology? Is a data provider's sole authority only limited to API technology that the data provider has deployed? Thus, if a patient requests that an app of their choice is deployed to access the patient’s EHI, the API Data Provider must use that app unless an exception to information blocking applies (e.g., the app presents a security risk).

As a part of the Condition and Maintenance of Certification for APIs, ONC proposes that an API Technology Supplier must public all terms and conditions needed to use any EHI that is obtained by means of the API technology. Due to the privacy concerns laid out above, AMA recommends that these terms and conditions needed to use EHI include patient consent and an explicit description as to how an individual’s data will be used.

VII.B.5 Real World Testing

§ 170.405 Real world testing

(a) Condition of Certification. A health IT developer with Health IT Modules to be certified to any one or more 2015 Edition certification criteria in § 170.315(b), (c)(1) through (3), (e)(1), (f), (g)(7) through (11), and (h) must successfully test the real world use of those Health IT Module(s) for interoperability (as defined in 42 U.S.C.300jj(9) and § 170.102) in the type of setting in which such Health IT Module(s) would be/is marketed.

(b) Maintenance of Certification.

(1) Real world testing plan submission. A health IT developer must submit an annual real world testing plan to its ONC-ACB via a publicly accessible hyperlink no later than December 15 of each calendar year for each of its certified 2015 Edition Health IT Modules that include certification criteria referenced in paragraph (a) of this section.

(i) The plan must be approved by a health IT developer authorized representative capable of binding the health IT developer for execution of the plan and include the representative's contact information.

(ii) The plan must include all health IT certified to the 2015 Edition through August 31st of the preceding year.

(ii) The plan must address the following for each of the certification criteria identified in paragraph (a) of this section that are included in the Health IT Module's scope of certification:

(A) The testing method(s)/methodology(ies) that will be used to demonstrate real world interoperability and conformance to the certification criteria's requirements, including scenario- and use case-focused testing;

(B) The care setting(s) that will be tested for real world interoperability and an explanation for the health IT developer's choice of care setting(s) to test;

(C) The timeline and plans for any voluntary updates to standards and implementation specifications that the National Coordinator has approved through the Standards Version Advancement Process.

(D) A schedule of key real world testing milestones;

(E) A description of the expected outcomes of real world testing;

(F) At least one measurement/metric associated with the real world testing; and

(G) A justification for the health IT developer's real world testing approach.

(2) Real world testing results reporting. A health IT developer must submit real world testing results to its ONC-ACB via a publicly accessible hyperlink no later than January 31 each calendar year for each of its certified 2015 Edition Health IT Modules that include certification criteria referenced in paragraph (a) of this section. The real world testing results must report the following for each of the certification criteria identified in paragraph (a)of this section that are included in the Health IT Module's scope of certification:

(i) The method(s) that was used to demonstrate real world interoperability;

(ii) The care setting(s) that was tested for real world interoperability;

(iii) The voluntary updates to standards and implementation specifications that the National Coordinator has approved through the Standards Version Advancement Process.

§ 170.405 Real world testing

(iv) A list of the key milestones met during real world testing;

(v) The outcomes of real world testing including a description of any challenges encountered during real world testing; and

(vi) At least one measurement/metric associated with the real world testing.

(3) USCDI Updates for C-CDA. A health IT developer with health IT certified to § 170.315(b)(1), (e)(1), (g)(6), (f)(5), and/or (g)(9) prior to the effective date of this final rule must:

(i) Update their certified health IT to be compliant with the revised versions of these criteria adopted in this final rule; and

(ii) Provide its customers of the previously certified health IT with certified health IT that meets paragraph (b)(3)(i) of this section within 24 months of the effective date of this final rule.

(4) C-CDA Companion Guide Updates. A health IT developer with health IT certified to § 170.315(b)(1), (b)(2), (b)(9), (e)(1), (g)(6), and/or (g)(9) prior to the effective date of this final rule must:

(i) Update their certified health IT to be compliant with the revised versions of these criteria adopted in this final rule; and

(ii) Provide its customers of the previously certified health IT with certified health IT that meets paragraph (b)(4)(i) of this section within 24 months of the effective date of this final rule.

(5) Voluntary standards and implementation specifications updates. A health IT developer subject to paragraph (a) of this section that voluntary updates its certified health IT to a new version of an adopted standard that is approved by the National Coordinator through the Standards Version Advancement Process must:

(i) Provide advance notice to all affected customers and its ONC-ACB –

(A) Expressing its intent to update the software to the more advanced version of the standard approved by the National Coordinator;

(B) The developer's expectations for how the update will affect interoperability of the affected Health IT Module as it is used in the real world;

(C) Whether the developer intends to continue to support the certificate for the existing certified Health IT Module version for some period of time and how long or if the existing certified Health IT Module version will be deprecated; and

(ii) Successfully demonstrate conformance with approved more recent versions of the standard(s) or implementation specification(s) included in applicable 2015 Edition certification criterion specified in paragraph (a) of this section.

Preamble FR Citation: 84 FR 7495-97 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Please see 84 FR 7578-82 for estimates related to this proposal.

Public Comment Field:

The AMA strongly supports the requirement for real-world testing as mandated by the Cures Act and generally as proposed by ONC. We agree with ONC that required testing should be limited to health IT

developers with Health IT Modules certified to one or more 2015 Edition certification criteria focused on interoperability and data exchange.
To improve on these requirements, the AMA recommends ONC by providing more clarity around what care settings/venues are covered by test plans, making minimum expectations clear, and establishing which settings and the number of settings that are applicable for certified Health IT Modules. We recommend ONC provide guidelines for a test plan.

We support the proposed pilot year. After the pilot year, we suggest the creation of a standardized template incorporating the elements of an acceptable test plan. ONC should provide clarity on measuring successful real word testing for the following: (1) continued compliance with certification criteria (including standards and code sets), (2) exchange within intended settings, and (3) receipt and use of electronic health information in the certified EHR. We recognize not all three elements are possible for all certification criteria proposed for real world testing.

The AMA recommends ONC clarify and define the terms, "scenario" and "use case". We also recommend ONC clarify the term "workflow". We acknowledge the variability that exists in physician workflows and is concerned this could require an infinite number of test cases for a health IT developer's customer base. We recommend ONC be clear and reasonable with what is intended where the preamble states "...developers can and should design scenario-based test cases that incorporate multiple functionalities as appropriate for the real world workflow and setting." ONC should clarify where existing interoperability testing (such as that performed by The Sequoia Project or other existing networks) can satisfy expectations for real world testing.

The use of information is important to usability of interoperability. Testing the use of information received through exchange requires consideration of human factors and usability to understand whether the intended users can efficiently and effectively use the presented information. If health IT developers are testing the use of data received through exchange, the health IT vendors should have users involved in the testing to validate that users can process and use that information. When certified health IT products receive "foreign" data it must be viewable, actionable, and reportable alongside the user's "native" data to be useful and reduce burden on physicians using the technology. Real world testing should reflect this requirement.

The AMA recommends ONC include a description of "measurement" and provide clarity on the role of measurement—specificity for purpose or proof points. ONC should consider including updated metric expectations after the pilot year. Where real world testing is for both interoperability and use of received data, the ONC should consider specifying that there be at least one metric for interoperability and one metric for use. For instance, ONC could include the number of "clicks" it takes to perform an action (e.g., order an MRI) and include the number of clicks it takes to perform a health information exchange operation (e.g., reconciliation of USCDI data elements).

We also support the Standards Version Advancement Process (SVAP) as enabling needed industry flexibility. We view the ONC certification program as providing a floor that all certified technology will need to support, while the SVAP provides permissible progressions (that later can become the new floor in the next rule). With respect to the SVAP's ability to assert conformance in the absence of the test tools, there is a need to test once tools become available. ONC should provide more clarity when a version of standards is available under this process but does not yet have testing tools available to determine conformance. It is fairly clear vendors must factor all claimed versions of standards into their real world testing, but ONC should clarify how the health IT developers are to address new versions for which tooling does not exist. ONC should clarify whether testing will be required in a subsequent year's real world testing plan once tooling is available or whether the health IT developer's previous attestation is sufficient.

VII.B.6 Attestations

§ 170.406 Attestations

(a) Condition of Certification. A health IT developer must provide the Secretary with an attestation of compliance with the Conditions and Maintenance of Certification requirements specified in §§ 170.401 through 170.405 at the time of certification. Specifically, a health IT developer must attest to:

(1) Having not taken any action that constitutes information blocking as defined in 42 U.S.C. 300jj-52 and § 171.103;

(2) Having provided assurances satisfactory to the Secretary that they will not take any action that constitutes information blocking as defined in 42 U.S.C. 300jj-52 and § 171.103, unless for legitimate purposes specified by the Secretary; or any other action that may inhibit the appropriate exchange, access, and use of electronic health information;

(3) Not prohibiting or restricting the communications regarding—

(i) The usability of its health IT;

(ii) The interoperability of its health IT;

(iii) The security of its health IT;

(iv) Relevant information regarding users' experiences when using its health IT;

(v) The business practices of developers of health IT related to exchanging electronic health information; and

(vi) The manner in which a user of the health IT has used such technology; and

(4) Having published application programming interfaces (APIs) and allowing health information from such technology to be accessed, exchanged, and used without special effort through the use of application programming interfaces or successor technology or standards, as provided for under applicable law, including providing access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws;

(5) Ensuring that its health IT allows for health information to be exchanged, accessed, and used, in the manner described in paragraph (a)(4) of this section; and

(6) Having undertaken real world testing of its Health IT Module(s) for interoperability (as defined in 42 U.S.C.300jj(9)) in the type of setting in which such Health IT Module(s) will be/is marketed.

(b) Maintenance of Certification.

(1) A health IT developer must attest to compliance with §§ 170.401 through 170.405 at the time of certification.

(2) A health IT developer must attest semiannually to compliance with §§ 170.401 through 170.405 for all its health IT that had an active certification at any time under the ONC Health IT Certification Program during the prior six months.

Preamble FR Citation: 84 FR 7501-02 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Please see 84 FR 7582-38 for estimates related to this proposal.

§ 170.406 Attestations

Public Comment Field:

The AMA supports these requirements. Physicians participating in the Quality Payment Program are already required to attest to a three-part information blocking statement. This statement is detailed and ties a physician's attestation to their EHR vendor's capabilities. For instance, physicians must attest they "implemented in a manner that allowed for the timely, secure, and trusted bidirectional exchange of structured electronic health information with other health care providers (as defined by 42 U.S.C. 300jj(3)), including unaffiliated providers, and with disparate CEHRT and health information technology (HIT) vendors." This is clearly technical and outside the control of most physicians. Alignment of expectations and requirements across stakeholders is necessary to ensure information blocking is curtailed. HHS should also strive for consistent policies to limit confusion. The AMA recommends ONC require EHR vendors to be held accountable for the same three requirements.

VII.D Enforcement

§ 170.580 ONC review of certified health IT or a health IT developer's actions

(a) * * *

(1) Purpose. ONC may directly review certified health IT or a health IT developer's actions or practices to determine whether either conform to the requirements of the ONC Health IT Certification Program.

(2) * * *

(i) Certified health IT causing or contributing to unsafe conditions. * * *

* * * * *

(ii) Impediments to ONC-ACB oversight of certified health IT. * * *

* * * * *

(iii) Noncompliance with Conditions and Maintenance of Certification. ONC may initiate direct review under this section if it has a reasonable belief that a health IT developer has not complied with a Condition or Maintenance of Certification requirement under subpart D of this part.

(3) * * *

(i) ONC's review of certified health IT or a health IT developer's actions or practices is independent of, and may be in addition to, any surveillance of certified health IT conducted by an ONC-ACB.

(4) Coordination with the Office of Inspector General.

(i) ONC may coordinate its review of a claim of information blocking with the Office of Inspector General or defer to the Office of Inspector General to lead a review of a claim of information blocking.

(ii) ONC may rely on Office of Inspector General findings to form the basis of a direct review action.

* * * * *

(iv) An ONC-ACB and ONC-ATL shall provide ONC with any available information that ONC deems relevant to its review of certified health IT or a health IT developer’s actions or practices.

(v) ONC may end all or any part of its review of certified health IT or a health IT developer’s actions or practices under this section at any time and refer the applicable part of the review to the relevant ONC-ACB(s) if ONC determines that doing so would serve the effective administration or oversight of the ONC Health IT Certification Program.

(b) * * *

(1) * * *

§ 170.580 ONC review of certified health IT or a health IT developer’s actions

(i) Circumstances that may trigger notice of potential non-conformity. At any time during its review of certified health IT or a health IT developer’s actions or practices under paragraph (a) of this section, ONC may send a notice of potential non-conformity if it has a reasonable belief that certified health IT or a health IT developer may not conform to the requirements of the ONC Health IT Certification Program.

* * * * *

(iii) * * *

(D) Issue a notice of proposed termination if the health IT is under review in accordance with paragraphs (a)(2)(i) or (ii) of this section.

(2) * * *

(i) Circumstances that may trigger notice non-conformity. At any time during its review of certified health IT or a health IT developer’s actions or practices under paragraph (a) of this section, ONC may send a notice of non-conformity to the health IT developer if it determines that certified health IT or a health IT developer’s actions or practices does not conform to the requirements of the ONC Health IT Certification Program.

* * * * *

(3) * * *

(i) All records related to the development, testing, certification, implementation, maintenance and use of its certified health IT;

(ii) Any complaint records related to the certified health IT;

(iii) All records related to the Condition(s) and Maintenance of Certification requirements, including marketing and distribution records, communications, and contracts; and

(iv) Any other relevant information.

(c) * * *

(1) Applicability. If ONC determines that certified health IT or a health IT developer’s action or practice does not conform to requirements of the ONC Health IT Certification Program, ONC shall notify the health IT developer of its determination and require the health IT developer to submit a proposed corrective action plan.

* * * * *

(e) * * *

(1) Applicability. Excluding situations of noncompliance with a Condition or Maintenance of Certification requirement under subpart D of this part, ONC may propose to terminate a certification issued to a Health IT Module if:

* * * * *

(f) * * *

(1) Applicability. The National Coordinator may terminate a certification if:

(i) A determination is made that termination is appropriate after considering the information provided

§ 170.580 ONC review of certified health IT or a health IT developer’s actions

by the health IT developer in response to the proposed termination notice;

(ii) The health IT developer does not respond in writing to a proposed termination notice within the timeframe specified in paragraph (e)(3) of this section; or

(iii) A determination is made that the health IT developer is noncompliant with a Condition or Maintenance of Certification requirement under subpart D of this part or for the following circumstances when ONC exercises direct review under paragraph (a)(2)(iii) of this section:

(A) The health IT developer fails to timely respond to any communication from ONC, including, but not limited to:

~~(1)~~ Fact-finding;

~~(2)~~ A notice of potential non-conformity within the timeframe established in accordance with paragraph (b)(1)(ii)(A)(3) of this section; or

~~(3)~~ A notice of non-conformity within the timeframe established in accordance with paragraph (b)(2)(ii)(A)(3) of this section.

(B) The information or access provided by the health IT developer in response to any ONC communication, including, but not limited to: fact-finding, a notice of potential non-conformity, or a notice of non-conformity is insufficient or incomplete;

(C) The health IT developer fails to cooperate with ONC and/or a third party acting on behalf of ONC;

(D) The health IT developer fails to timely submit in writing a proposed corrective action plan;

(E) The health IT developer fails to timely submit a corrective action plan that adequately addresses the elements required by ONC as described in paragraph (c) of this section;

(F) The health IT developer does not fulfill its obligations under the corrective action plan developed in accordance with paragraph (c) of this section; or

(G) ONC concludes that the non-conformity(ies) cannot be cured.

* * * * *

(g) * * *

(1) Basis for appeal. A health IT developer may appeal an ONC determination to suspend or terminate a certification issued to a Health IT Module and/or an ONC determination to issue a certification ban under § 170.581(a)(2) if the health IT developer asserts:

(i) ONC incorrectly applied ONC Health IT Certification Program requirements for a

(A) Suspension;

(B) Termination; or

(C) Certification ban under § 170.581(a)(2); or

* * * * *

(2) Method and place for filing an appeal. A statement of intent to appeal followed by a request for appeal must be submitted to ONC in writing by an authorized representative of the health IT developer subject to the determination being appealed. The statement of intent to appeal and request for appeal must be filed in accordance with the requirements specified in the notice of:

§ 170.580 ONC review of certified health IT or a health IT developer's actions

(i) Termination;

(ii) Suspension; or

(iii) Certification ban under § 170.581(a)(2).

(3) * * *

(i) A statement of intent to appeal must be filed within 10 days of a health IT developer's receipt of the notice of:

(A) Suspension;

(B) Termination; or

(C) Certification ban under § 170.581(a)(2).

* * * * *

(4) Effect of appeal.

(i) A request for appeal stays the termination of a certification issued to a Health IT Module, but the Health IT Module is prohibited from being marketed, licensed, or sold as "certified" during the stay.

(ii) A request for appeal does not stay the suspension of a Health IT Module.

(iii) A request for appeal stays a certification ban issued under § 170.581(a)(2).

(5) * * *

(i) The hearing officer may not review an appeal in which he or she participated in the initial suspension, termination, or certification ban determination or has a conflict of interest in the pending matter.

* * * * *

(6) * * *

(v) ONC will have an opportunity to provide the hearing officer with a written statement and supporting documentation on its behalf that clarifies, as necessary, its determination to suspend or terminate the certification or issue a certification ban.

* * * * *

Preamble FR Citation: 84 FR 7503-07 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Please see 84 FR 7583-84 for estimates related to this proposal.

Public Comment Field:

The AMA supports these requirements.

§ 170.505 Correspondence

(a) Correspondence and communication with ONC or the National Coordinator shall be conducted by email, unless otherwise necessary or specified. The official date of receipt of any email between ONC or the National Coordinator and an applicant for ONC-ACB status, an applicant for ONC-ATL status, an ONC-ACB, an ONC-ATL, health IT developer, or a party to any proceeding under this subpart is the date on which the email was sent.

(b) In circumstances where it is necessary for an applicant for ONC-ACB status, an applicant for ONC-ATL status, an ONC-ACB, an ONC-ATL, health IT developer, or a party to any proceeding under this subpart to correspond or communicate with ONC or the National Coordinator by regular, express, or certified mail, the official date of receipt for all parties will be the date of the delivery confirmation to the address on record.

Preamble FR Citation: 4 FR 7503-04 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

The AMA supports these requirements.

§ 170.581 Certification ban

(a) Circumstances trigger a certification ban. The certification of any of a health IT developer's health IT is prohibited when:

(1) The certification of one or more of the health IT developer's Complete EHRs or Health IT Modules is:

(i) Terminated by ONC under the ONC Health IT Certification Program;

(ii) Withdrawn from the ONC Health IT Certification Program by an ONC-ACB because the health IT developer requested it to be withdrawn when the health IT developer's health IT was the subject of a potential non-conformity or non-conformity as determined by ONC;

(iii) Withdrawn by an ONC-ACB because of a non-conformity with any of the certification criteria adopted by the Secretary under subpart C of this part;

(iv) Withdrawn by an ONC-ACB because the health IT developer requested it to be withdrawn when the health IT developer's health IT was the subject of surveillance for a certification criterion or criteria adopted by the Secretary under subpart C of this part, including notice of pending surveillance; or

(2) ONC determines a certification ban is appropriate per its review under § 170.580(a)(2)(iii).

(b) Notice of certification ban. When ONC decides to issue a certification ban to a health IT developer, ONC will notify the health IT developer of the certification ban through a notice of certification ban. The notice of certification ban will include, but may not be limited to:

§ 170.581 Certification ban

(1) An explanation of the certification ban;

(2) Information supporting the certification ban;

(3) Instructions for appealing the certification ban if banned in accordance with paragraph (a)(2) of this section; and

(4) Instructions for requesting reinstatement into the ONC Health IT Certification Program, which would lift the certification ban.

(c) Effective date of certification ban.

(1) A certification ban will be effective immediately if banned under paragraphs (a)(1) of this section.

(2) For certification bans issued under paragraph (a)(2) of this section, the ban will be effective immediately after the following applicable occurrence:

(i) The expiration of the 10-day period for filing a statement of intent to appeal in § 170.580(g)(3)(i) if the health IT developer does not file a statement of intent to appeal.

(ii) The expiration of the 30-day period for filing an appeal in § 170.580(g)(3)(ii) if the health IT developer files a statement of intent to appeal, but does not file a timely appeal.

(iii) A final determination to issue a certification ban per § 170.580(g)(7) if a health IT developer files an appeal timely.

(d) Reinstatement. The certification of a health IT developer's health IT subject to the prohibition in paragraph (a) of this section may commence once the following conditions are met.

(1) A health IT developer must request ONC's permission in writing to participate in the ONC Health IT Certification Program.

(2) The request must demonstrate that the customers affected by the certificate termination, certificate withdrawal, or non-compliance with a Condition or Maintenance of Certification have been provided appropriate remediation.

(3) For non-compliance with a Condition or Maintenance of Certification requirement, the non-compliance must be resolved.

(4) ONC is satisfied with the health IT developer's demonstration under paragraph (d)(2) of this section that all affected customers have been provided with appropriate remediation and grants reinstatement into the ONC Health IT Certification Program.

Preamble FR Citation: 84 FR 7504-06 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

The AMA recognizes instances where banning certified health IT may be justified. However, banning may severely impact physicians whose EHRs may become banned with no fault to the physician. ONC should coordinate with CMS to extend their hardship exceptions for physicians whose EHR products become banned similar to how ONC currently coordinated with CMS regarding terminated CEHRT.

§ 171.102 Definitions

For purposes of this part:

Access means the ability or means necessary to make electronic health information available for use, including the ability to securely and efficiently locate and retrieve information from any and all source systems in which the information may be recorded or maintained.

Actor means a health care provider, health IT developer of certified health IT, health information exchange, or health information network.

API Data Provider is defined as it is in § 170.102.

API Technology Supplier is defined as it is in § 170.102.

Electronic Health Information (EHI) means—

(1) Electronic protected health information; and

(2) Any other information that identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual and is transmitted by or maintained in electronic media, as defined in 45 CFR 160.103, that relates to the past, present, or future health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Electronic media is defined as it is in 45 CFR 160.103.

Electronic protected health information (ePHI) is defined as it is in 45 CFR 160.103.

§ 171.102 Definitions

~~Exchange~~ means the ability for electronic health information to be transmitted securely and efficiently between and among different technologies, systems, platforms, or networks in a manner that allows the information to be accessed and used. Fee means any present or future obligation to pay money or provide any other thing of value.

~~Health care provider~~ has the same meaning as ‘‘health care provider’’ at 42 U.S.C. 300jj.

~~Health Information Exchange or HIE~~ means an individual or entity that enables access, exchange, or use of electronic health information primarily between or among a particular class of individuals or entities or for a limited set of purposes.

~~Health Information Network or HIN~~ means an individual or entity that satisfies one or both of the following—

(1) Determines, oversees, administers, controls, or substantially influences policies or agreements that define business, operational, technical, or other conditions or requirements for enabling or facilitating access, exchange, or use of electronic health information between or among two or more unaffiliated individuals or entities.

(2) Provides, manages, controls, or substantially influences any technology or service that enables or facilitates the access, exchange, or use of electronic health information between or among two or more unaffiliated individuals or entities.

~~Health IT developer of certified health IT~~ means an individual or entity that develops or offers health information technology (as that term is defined in 42 U.S.C. 300jj(5)) and which had, at the time it engaged in a practice that is the subject of an information blocking claim, health information technology (one or more) certified under the ONC Health IT Certification Program.

~~Information blocking~~ is defined as it is in § 171.103 and 42 U.S.C. 300jj-52(a).

~~Interfere with~~ means to prevent, materially discourage, or otherwise inhibit access, exchange, or use of electronic health information.

~~Interoperability element~~ means—

(1) Any functional element of a health information technology, whether hardware or software, that could be used to access, exchange, or use electronic health information for any purpose, including information transmitted by or maintained in disparate media, information systems, health information exchanges, or health information networks.

(2) Any technical information that describes the functional elements of technology (such as a standard, specification, protocol, data model, or schema) and that a person of ordinary skill in the art may require to use the functional elements of the technology, including for the purpose of developing compatible technologies that incorporate or use the functional elements.

(3) Any technology or service that may be required to enable the use of a compatible technology in production environments, including but not limited to any system resource, technical infrastructure, or health information exchange or health information network element.

(4) Any license, right, or privilege that may be required to commercially offer and distribute compatible technologies and make them available for use in production environments.

§ 171.102 Definitions

(5) Any other means by which electronic health information may be accessed, exchanged, or used.

Permissible purpose means a purpose for which a person is authorized, permitted, or required to access, exchange, or use electronic health information under applicable law.

Person is defined as it is in 45 CFR 160.103.

Protected health information is defined as it is in 45 CFR 160.103.

Practice means one or more related acts or omissions by an actor.

Use means the ability of health IT or a user of health IT to access relevant electronic health information; to comprehend the structure, content, and meaning of the information; and to read, write, modify, manipulate, or apply the information to accomplish a desired outcome or to achieve a desired purpose.

Preamble FR Citation: 84 FR 7509-15 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

The AMA strongly supports the elimination of unjustified information blocking that prevents data exchange. ONC needs to prohibit networks, exchanges, developers, and other health care providers from blocking the electronic availability of clinical data to health care providers who participate in the care of shared patients. Information blocking under these circumstances interferes with the provision of optimal, safe, and timely care. While we support the prohibition on information blocking, the AMA has concerns regarding the broad definition of terms and seeks clarification as to ONC's interpretation.

OVERALL DEFINITIONAL ISSUES

The proposed Part 171 Information Blocking contains definitions for terms such as electronic health information, information blocking, access, use, and exchange that are used throughout Part 171. These terms are also used in proposed provisions in Part 170; however, Part 170 does not define these terms. As proposed, this lack of definitions creates the ability to have two separate interpretations of these terms depending on which part and introduces unnecessary vagueness and inconsistency. ONC could remedy this situation by defining these terms in Part 170 with regulatory language such as "is defined as it is in § 171.102 of this subchapter." However, ONC should be aware of any potential unintended consequences in applying these terms throughout Part 170. For example, with the proposed definition "use" having writing capability being extended to CEHRT requirements.

HEALTH INFORMATION NETWORK

The AMA strongly recommends that the definition of Health Information Network (HIN) be narrowed to include only entities that are an actual network (or formalized component of an actual network) and have an actual operational role and responsibility for the network. For example, to be a HIN, the network itself provides the ability to locate and transmit EHI between multiple persons and/or entities electronically, on demand, or pursuant to one or more automated processes. Moreover, to be a HIN, the entity should also be exchanging EHI in a live clinical environment using the network in some capacity. Thus, health care providers and organizations with limited exchange capabilities, such as interfaces for Admission, Discharge, and Transfer messages or lab results, should not be considered a HIN.

HINs typically operate as Business Associates and currently have Business Associate agreements in place with their participants who are Covered Entities. These agreements facilitate the exchange of EHI since they perform functions or activities on behalf of, or provide certain services for Covered Entities such as determining and administering policies or agreements that define business, operational, technical, or other conditions or requirements for enabling or facilitating access, exchange, or use of health information between or among two or more Covered Entities. Therefore, for example, organizations that develop voluntary standards and policies that may be used by a HIN should not be considered a HIN.

FUNCTIONAL ELEMENT

In defining "Interoperability Element", ONC states that the term is not limited to functional elements and technical information but also encompasses technologies, services, policies, and other conditions necessary to support the uses of EHI. ONC's intent is to capture the potential means by which EHI may be accessed, exchanged, and used. The AMA believes that Interoperability Element should not include the underlying substantive content because such content is not a potential means by which EHI may be accessed, exchanged, or used. Therefore, ONC should clarify that underlying substantive content is not included in the definition of Interoperability Element.

ELECTRONIC HEALTH INFORMATION

As previously mentioned, the AMA believes that the definition of EHI is too broad. We are also concerned about the impracticality of applying this subjective definition to the information blocking provisions to an extensive, highly situational and largely non-standardized data set. Instead, the AMA recommends alignment between ONC's information blocking provisions, EHI, and USCDI proposals could happen in several ways. The AMA is recommending two potential paths:

- ONC could constrain its definition of EHI to just the data elements represented by the USCDI for specified actors. Information blocking requirements would be subject to newly-scoped access, use, and exchange of the USCDI. Patients would retain their rights to request their designated record set as outlined by HIPAA (the Director of the HHS Office of Civil Rights has already noted publicly that patient access enforcement will increase this year). EHI export could be scoped to focus on ePHI as outlined by HIPAA. Additional data classes (e.g., payment and cost information) would propagate through the USCDI expansion process with support from the ISA and SVAP.

- Alternatively, ONC could retain its EHI definition, rescope the terms "access", "use", and "exchange", and include additional information blocking exceptions. ONC could establish an exception for actors only able to make the USCDI available. This exception should be concise, clear, implementable, and refrain from burdensome policy and procedure requirements. This could also be accomplished by modifying the proposed "Infeasibility of Request" exception. We encourage ONC to clarify that actors that do not comply with the request for access, exchange, or use of EHI, but that do comply to the best of their ability with requests for access, exchange, or use of the USCDI be able to claim this exception. Also, ONC should clarify that an actor could claim an exception for responding in "good faith" to requests beyond the USCDI.

UNREASONABLE

While information blocking applies to all actors under the statute, health care providers have different elements and penalties than developers, exchanges, and networks. For example, health care providers need to have specific intent that a practice is unreasonable to be considered an information blocker. Developers, exchanges, and networks do not need specific intent to be considered an information blocker nor have an element that requires HHS to determine that practice was unreasonable. Given these difference, the AMA recommends that ONC define "unreasonable" for purposes of information blocking (proposed 45 CFR

§ 171.103(c)) in subsequent rulemaking.

In defining "unreasonable," ONC should look to the MIPS Promoting Interoperability information blocking attestation.[13] Namely, that an unreasonable practice occurs when a health care provider does not act in good faith to exchange EHI in a health care provider's particular situation. This definition would recognize circumstances exist that are beyond a health care provider's control which may limit the exchange or use of EHI. Moreover, focusing on an individual provider's circumstances like practice or organization size can help set proper expectations that health care providers may not have any special technical skills or need to personally deal with the technical details of implementing health IT. Furthermore, defining unreasonable in this manner would help ONC implement its statutory mandate under Cures to ensure that health care providers are "not penalized for the failure of developers of [HIT] or other entities offering [HIT] to such providers to ensure that such technology meets the requirements to be certified."[14]

IDENTIFIABLE INDIVIDUAL

The AMA agrees that the definition of EHI should not include health information that is de-identified consistent with the requirements of 45 CFR § 164.514(b) because the main goal of the information blocking provision is to facilitate an individual's access to EHI. Information that does not identify an individual would not facilitate access of EHI to an individual. Thus, we recommend adding "identifiable individual" to the definitions of Access, EHI, Exchange, Health Information Exchange, and Use in proposed § 171.102. Adding identifiable individual will also help guard against potential overreach by entities making broad requests of EHI without referencing specific individuals. The proposed definitions should read as follows:

- *Access* means the ability or means necessary to make electronic health information <u>of an identifiable individual</u> available for use, including the ability to securely and efficiently locate and retrieve information from any and all source systems in which the information may be recorded or maintained.
- *Electronic Health Information (EHI)* means— Electronic protected health information; and Any other information that identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual and is transmitted by or maintained in electronic media, as defined in 45 CFR 160.103, that relates to the past, present, or future health or condition of an <u>identifiable</u> individual; the provision of health care to an <u>identifiable</u> individual; or the past, present, or future payment for the provision of health care to an <u>identifiable</u> individual.
- *Exchange* means the ability for electronic health information <u>of an identifiable individual</u> to be transmitted securely and efficiently between and among different technologies, systems, platforms, or networks in a manner that allows the information to be accessed and used.
- *Health Information Exchange* or *HIE* means an individual or entity that enables access, exchange, or use of electronic health information <u>of an identifiable individual</u> primarily between or among a particular class of individuals or entities or for a limited set of purposes.
- *Use* means the ability of health IT or a user of health IT to access relevant electronic health information; to comprehend the structure, content, and
- meaning of the information; and to read, write, modify, manipulate, or apply the information <u>of an identifiable individual</u> to accomplish a desired outcome or to achieve a desired purpose.

DEFINITION OF USE

The AMA believes that the definition of Use is too broad, inappropriately increases administrative burden, and will unintentionally make EHI less secure. As proposed, the definition of Use includes the ability to access relevant EHI to comprehend the structure, content, and meaning of information. Requiring and

[13] CMS, *Fact Sheet: The MIPS Promoting Interoperability Prevention of Information Blocking Attestation* (2019).
[14] 42 USC § 300jj-52(a)(7).

ensuring comprehension of EHI will add administrative burden because it will force health care providers to provide both relevant and irrelevant information and could take a physician's time away from patient care by forcing the physician to explain complex or irrelevant information to patients. Physicians need to encourage open communication with their patients; all patients—not just those with limited health literacy—can benefit from clear communication practices. As such, physicians and staff are well-versed in how to communicate key points and know how to avoid overwhelming a patient with information that may not be relevant to his or her care. Requiring physicians to flood patients with information and ensure understanding of all EHI, even EHI that is not in the control of an individual physician, or face harsh penalties represents an unwarranted intrusion into the physician-patient relationship.

Alternatively, ONC should define Use to include a good faith or reasonable standard of comprehension or require Use without the need for further translation or deciphering. Moreover, ONC should look to more established definitions of use for guidance, such as in HIPAA, where use means, in part, "with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information. . . ."

ONC's definitional ambiguity will require physicians to adjust their systems to permit "access", "exchange", and "use" of EHI in new ways—resulting in a series of "trial and error" scenarios and forcing EHR vendors and physicians to guess at what should be accessed or used and from whom. This could result in exposing multiple entry points to cyber attackers seeking to exploit vulnerabilities, which could be more numerous and expose more data than ever before given the amount of information ONC is proposing that actors share. These adversaries will target the weakest link in the chain, which may be a physician office or legacy technologies.

ONC's proposals may swing the pendulum from not sharing information to sharing everything and enabling unprecedented electronic access and modification to medical records. Professional societies representing practice administrators, health system chief information officers, and security professionals are already expressing apprehension.[15,16,17] Concerningly, they all sound alarms that EHRs will not sufficiently protect the "use" of EHI as envisioned by ONC.

There are major implications for EHI *use* as proposed by ONC. For one, **using EHI would allow an actor (e.g., a consumer-facing app developer) the ability to *read, write,* and *modify* a patient's entire medical record—including financial, demographic, genetic, protected SUD or mental health, and family information, in an EHR. This is a staggering shift from current EHR capabilities.** Not only are APIs and ONC's proposed API requirements woefully insufficient to protect bi-direction exchange of data, but security experts who participate in HHS advisory committees have themselves highlighted the need for major security and privacy controls to comply ONC's information blocking proposals.

[15] Health IT Security, *As ONC Considers Info Blocking, IoT, Medical Device Guidance Needed*, April 2019, available at: https://healthitsecurity.com/news/as-onc-considers-info-blocking-iot-medical-device-guidance-needed?eid=CXTEL000000154738&elqCampaignId=9253&elqTrackId=151c5e0bac4b4df6b2155ef6a9ffce20&elq=9d083122ab044763baa6817a857a7474&elqaid=9715&elqat=1&elqCampaignId=9253

[16] Fierce Healthcare, *Complying with information blocking rule will be a challenge without standardized APIs: HIMSS*, March 2019, available at: https://www.fiercehealthcare.com/tech/complying-information-blocking-rule-will-be-a-challenge-without-standardized-apis-himss

[17] Health IT Security, *ONC Information Blocking Rule Raises Privacy and Security Concerns*, March 2019, available at: https://healthitsecurity.com/news/onc-information-blocking-rule-raises-privacy-and-security-concerns?eid=CXTEL000000154738&elqCampaignId=8938&elqTrackId=7b46f9fd83434ed99efae92be850fefd&elq=89d147ceb6e246fd99eed1ba66e334b3&elqaid=9402&elqat=1&elqCampaignId=8938

> *Before enacting the information blocking rule, ONC should first consider selecting or establishing a security controls framework for interoperability and data sharing processes that would support the trusted environments necessary "to build confidence in payers, providers, and patients."*[18,19]

Furthermore, Christopher Wray, the Director of the U.S. Federal Bureau of Investigation (FBI), announced in March 2019 that, "Today's cyberthreat is bigger than any one government agency—in fact it's bigger than the government itself," and that "the scope, breadth, depth, sophistication and diversity of the threat we face now is unlike anything we've had in our lifetimes."[20] These circumstances raise numerous questions:

- **Has ONC established a security controls framework for interoperability and data sharing?**
- **How will ONC, a single government agency, ensure EHI access, exchange, and use does not compromise the personal health information of U.S. citizens?**
- **What is ONC's plan to ensure that thousands of apps properly authenticate for EHI use?**
- **What is ONC's plan for protecting the multiple access points and attack surfaces that will be necessary to facilitate EHI use?**
- **How is ONC going to ensure EHR vendors develop and test to security industry protective measures, prescribed standards, and security protocols?**

The federal government needs to empower physicians to actively manage their security posture, not hinder them**.** We seek clarity from ONC as to whether it expects physicians to use information blocking exceptions and documentation as "protection" from these risks.

[18] Id.

[19] CynergisTek is represented on The Healthcare and Public Health Sector Coordinating Council (HSCC).

[20] Healthcare IT News, *RSA 2019: FBI Director Christopher Wray says 'today's cybersecurity threat is bigger than government itself*', March 2019, available at: https://www.healthcareitnews.com/news/rsa-2019-fbi-director-christopher-wray-says-today%E2%80%99s-cybersecurity-threat-bigger-government?mkt_tok=eyJpIjoiTWpjd05HRmtZV0V3WW1OaiIsInQiOiJYN2Q0dVhtQUxHRytncTl1NlZSWXdlekZCSWpMU3hoUmFqZlwvdzBacTBZTjBrR1hWZmlRYWlkc1VpV0RhdE9xWUc5VjF0TDFZNGo2TnV6VG1aZlRndGd6SXRoTFFVWTFUV3Zqdm5YUVNhWUhsSm9ua2tHV1wvTWEwY0hWWHBLN1N1In0%3D

Request for comment regarding price information (ONC)

We seek comment on the parameters and implications of including price information within the scope of EHI for purposes of information blocking.

Preamble FR Citation: 84 FR 7513-14 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

The lack of complete, accurate, and timely information about the cost of health care services prevents health care markets from operating efficiently. As the health care market evolves, patients increasingly are becoming active consumers of health care services. Achieving meaningful price transparency can help lower health care costs and empower patients to make informed care decisions. The AMA supports price transparency and recognizes that achieving meaningful price transparency may help control health care costs by helping patients to choose low-cost, high-quality care.

The AMA supports the following specific measures to expand the availability of health care pricing information that allows patients and their physicians to make value-based decisions when patients have a choice of provider or facility:

- Patient confusion and health literacy should be addressed by developing resources that help patients understand the complexities of health care pricing and encourage them to seek information regarding the cost of health care services they receive or anticipate receiving.
- All health care professionals and entities should be required to make information about prices for common procedures or services readily available to consumers.
- Physicians should communicate information about the cost of their professional services to individual patients, taking into consideration the insurance status of the patient (e.g., self-pay, in-network insured, out-of-network insured) where possible.
- Health plans should provide plan enrollees or their designees with complete information regarding plan benefits and real-time, cost-sharing information associated with both in-network and out-of-network provider services or other plan designs that may affect patient out-of-pocket costs.
- Health plans, public and private entities, and other stakeholder groups should work together to facilitate price and quality transparency for patients and physicians.
- Entities promoting price transparency tools should have processes in place to ensure the accuracy and relevance of the information they provide.
- All-payer claims databases should be supported and strengthened.
- Electronic health records (EHR) vendors should include features that assist in facilitating price transparency for physicians and patients.

Pricing Information in EHI

The AMA fully supports price transparency. However, we believe that defining EHI to include various types of price information and then holding physicians and other entities accountable under the information blocking provisions is inappropriate because this pricing information is generally held and controlled by health plans. These plans are not subject to the information blocking provisions and therefore do not have the same incentives to share information.

The lack of transparency in health care pricing and costs is primarily the result of a health care financing system that depends largely on the complex arrangements between and among employers, third-party payers, providers, and patients. These arrangements can make it difficult to identify accurate and relevant information regarding costs associated with specific medical services and procedures. For example, contracts offered by payers to providers frequently delineate contracted rates as proprietary information. Insurer payment policies, coverage rules, and cost-sharing requirements are difficult to communicate in a common manner. Moreover, determining whether a provider is in-network may be difficult because of outdated provider directories or confusion associated with multiple plan contracts. Price also varies depending on where the service is performed, which impacts cost and a patient's cost-sharing. The cumulative effects of each of these factors often make it difficult to provide accurate pricing information for an individual patient in the absence of an actual service claim.

Reasonably Available at Point of Sale

An ideal price transparency system would allow patients to access relevant and accurate information prior to receiving care. This would enable patients to anticipate their potential costs in advance, and to choose among providers to seek the best value care. Yet, anticipating the need for health care services is often difficult. The urgent nature of some medical care, the inability to predict the particular course of treatment that might be indicated or identified subsequent to the initial complaint, and the intensity and scope of service required often leave patients without time or ability to evaluate their options prior to receiving care.

Reference Price as a Comparison Tool

The AMA does not object to using a reference price as a comparison. This price should be set at a level that reflects current market conditions and ensures that patients have access to a choice of providers. Prices should be reviewed annually and adjusted as necessary based on changes in market conditions.

However, **AMA strongly objects to the use of Medicare as a comparison rate**. Medicare payment rates do not reflect the costs of providing care, especially in the commercial market where the population varies greatly. Medicare uses the resource-based relative value scale (RBRVS) system to establish physician payments, determined by the resource costs associated with the total amount of physician resources required to provide a specific service.

Yet, before Medicare rates are finalized, they go through adjustment and conversion processes to meet federal budgetary requirements. Adjustments are done in a budget neutral manner, meaning that if an adjustment increases the payment for one service, it must account for this increase by decreasing payment in another. This establishes artificial decreases in payment for many physician services ever year. And before the final Medicare payment is set, geographically adjusted values are multiplied by a conversion factor - a monetary payment determined by Medicare each year that changes based on the Medicare economic index, adjustments pertaining to budget neutrality and other adjustments stipulated by legislation. After everything is complete, the resulting payment rates are not reflective of markets rates for physician services. For example, according to CMS, Medicare reimbursement covers less than 60% of direct Practice Expense costs in 2019.[21] Therefore, we strongly object to the use of Medicare as a comparison tool.

[21] CMS, Revisions to Payment Policies under the Medicare Physician Fee Schedule, Quality Payment Program and Other Revisions to Part B for CY 2019, CMS-1693-F CY 2019 PFS Final Rule Calculation of PE RVUs under Methodology for Selected Codes, https://www.cms.gov/Medicare/Medicare-Fee-for-Service-Payment/PhysicianFeeSched/PFS-Federal-Regulation-Notices-Items/CMS-1693-F.html.

Instead, the reference price for comparison should be an initiative led by a nonprofit entity which already have information available that can be used to help consumers obtain general price estimates of medical care. For example, on the FAIR Health website, consumers can search for in- and out-of-network prices for specific medical services or episodes of care within their geographic region.

EHR Vendors and Price Information

The AMA believes that EHR vendors can support the availability of price information by including features that assist in facilitating price transparency for physicians and patients. In an ideal world, the AMA believes that health IT developers should include in their platforms a mechanism for patients to see price information and for health care providers to also have access to information. As mentioned by ONC, this price information must be integrated into the practice or clinical workflow.

Timing of Price Information

As mentioned above, anticipating the need for health care services is often difficult. The urgent nature of some medical care, the inability to predict the particular course of treatment that might be indicated or identified subsequent to the initial complaint, and the intensity and scope of service required often leave patients without time or ability to evaluate their options prior to receiving care. Even scheduled care may prove difficult because a visit may result unanticipated orders or tests.

The AMA strongly supports education of the public about the costs associated with inappropriate use of emergency transportation services including ground and air services. However, the discussion of costs is precluded at the point of care in the case of emergencies under the Emergency Medical Treatment and labor Act (EMTALA),[22] and we continue to support this prohibition.

Price Information and Type of Health Insurance

The AMA recognizes that accurate cost information for consumers is tied to consumers' insurance, or lack thereof. Consumers who are insured, whether through private insurance, Medicare, or Medicaid, may face different costs for the same health care item or service (prescription drugs, physician services, hospital services, medical testing, etc.), depending upon their specific insurance plan although that is not always a guarantee of what the patient's plan will cover. Generally, insured consumers can best learn about cost by contacting their insurance provider. The AMA notes that consumers, regardless of insurance status, sometimes also turn to their respective health care provider for information on prices and out-of-pocket costs. Physicians and other providers can communicate information about the cost of their professional services to individual patients, taking into consideration the insurance status (e.g., self-pay, in-network insured, out-of-network insured) of the patient or other relevant information where possible. Uninsured consumers are especially reliant on information provided to them by hospitals, physicians, pharmacies, and other stakeholders.

The AMA believes that health plans should provide plan enrollees with complete information regarding plan benefits and real-time cost-sharing information associated with both in-network and out-of-network provider services or other plan designs that may affect a patient's out-of-pocket costs. A significant obstacle to price transparency and cost containment is complexity. Determining the exact services needed and comparing prices among providers is a challenge for many consumers and physicians, especially in light of significant price variation across site of service and within and across markets. It is difficult for consumers to identify relevant pricing information due to a wide variety of insurance benefit structures

[22] In 1986, Congress enacted the EMTALA to ensure public access to emergency services regardless of ability to pay. Section 1867 of the Social Security Act imposes specific obligations on Medicare-participating hospitals that offer emergency services to provide a medical screening examination when a request is made for examination or treatment for an emergency medical condition, including active labor, regardless of an individual's ability to pay. Hospitals are then required to provide stabilizing treatment for patients with emergency medical conditions.

and cost-sharing requirements. This challenge is exacerbated when a patient needs multiple services where it is difficult to ensure that every provider involved in the care is in-network and that every service is covered and determine at what cost. Though pricing tools may help identify in-network providers and estimate costs, they often lack consistency and should be standardized through uniform formatting. Providing consumers with meaningful, accurate, and readily-available price information will reduce costs and improve the health care system.

In addition to relying on health plans for pricing information, patients also rely on their physicians. To the extent price and quality information is available, physicians should engage in shared decision-making with their patients to communicate information about the cost of their professional services to individual patients taking into consideration the insurance status of the patient. The AMA believes that EHR vendors can support the availability of this information by including features that assist in facilitating price transparency for physicians and patients.

It also should be stated that the adequacy and accuracy of provider networks are essential to patients' informed decision-making. Patients need to be able to access all needed primary and specialty care within their insurance plan's provider network, and efforts by state and federal regulators to require insurers to meet objective network adequacy standards should continue. Moreover, provider directories are the tools with which patients may choose their health insurance product and determine which physicians and other providers to see for care. Inaccuracies in provider directors can have significant financial implications for patients. Therefore, the AMA strongly supports the proposal in the CMS rule to require that provider networks are up-to-date, accurate, and transparent.

Available Electronic Mechanisms

The AMA is confused by the terminology of "not in the provider system." As mentioned above, accurate cost information is tied to a patient's health plan. The health plan is in the best position to provides the cost sharing information given item or service, as the price they will pay depends on their specific plan, how much of their deductible has been met, the level of coinsurance and/or co-payment that may be required, and the setting where services are delivered.

Public Posting of Price Information

The AMA recognizes that stakeholders across the health care system have varying responsibilities and roles to play in providing pricing information to consumers. The responsibilities differ, however, based on whether patients are insured or uninsured.

For insured patients, health plans must provide plan enrollees or their designees with complete information regarding plan benefits and real-time cost-sharing information associated with both in-network and out-of-network provider services or other plan designs that may affect patient out-of-pocket costs. Such information must also be provided at the time of health plan enrollment to ensure patients have the information necessary to make informed health plan choices. Ultimately, health plans have the most accurate information necessary to share with their enrollees regarding the price they will pay, depending on their specific plan, how much of their deductible has been met, and the level of coinsurance and/or co-payment that may be required. For individuals with employer-sponsored coverage, employer human resources departments often augment the health benefits information provided to their employees. It is also imperative for third-party payers and purchasers to make such cost and pricing data available to physicians and other providers in a useable form at the point of service and decision-making, including the cost of each alternate intervention, and the insurance coverage and cost-sharing requirements of the respective patient. Specifically, PBMs, health insurers, and pharmacists should enable physicians to receive accurate, real-time formulary data at the point of prescribing.

For self-paying patients, physicians, hospitals, and other providers have a role to play in providing appropriate pricing information to patients. Physicians and other providers can communicate information about the cost of their professional services to individual patients, taking into consideration the insurance status (e.g., self-pay, in-network insured, out-of-network insured) of the patient or other relevant information where possible. The AMA believes that hospitals should adopt, implement, monitor, and publicize policies on patient discounts, charity care, and fair billing and collection practices, and make access to those programs readily available to eligible patients. Pharmacists must also inform patients of the cash prices of any medications they need.

Uninsured Rates

Uninsured rates like cash price may play a limited role in greater price transparency because the true out-of-pocket cost varies vastly from cash price because of the complexity of third-party payers including discounted fees, negotiated rates, use of in-network providers, deductibles, and co-payments. Even self-paying patients may have a different out-of-pocket cost from the cash price because the patient may receive charity care or prompt pay discounts.

The AMA recognizes that the term "cash price" typically refers to the price available to self-paying patients, outside of the scope of health insurance coverage. Discounted fees for insured patients originate from contracts that physicians, hospitals and other providers have with insurers. Prior to reaching an annual deductible, the majority of insured patients pay out-of-pocket for the full cost of their medical care, typically with access to the insurer's discounted fees. Upon reaching the deductible, most insured patients continue to be directly responsible for a portion of their medical bill—based again on discounted rates—in the form of co-payments or coinsurance.

Self-paying patients, however, pay directly for their medical services, and typically will not have access to the discounted fees of insurers for in-network physicians, hospitals and other providers. Alternatively, they pay the "cash price" for their respective medical service or prescription drug. Self-paying patients can seek the "cash prices" from their respective providers and pharmacies. Providers can communicate such information to individual patients, and hospitals can be encouraged to adopt, implement, monitor and publicize policies on patient discounts, charity care, and fair billing and collection practices, and make access to those programs readily available to patients.

Price Transparency and Value-Based Arrangements

To make value-based health care choices, consumers need pricing information paired with quality information. Consumers must be able to understand and anticipate costs by knowing the price and quality of services before receiving them to be able to choose high quality lower-cost services and providers. However, integrating meaningful cost and quality information in a useable format in transparency efforts is challenging. Aggravating this challenge is the fact that many health care services still lack relevant quality metrics. Studies indicate that patients are willing and able to make choices based on value as long as the information is presented clearly.

The methodologies used by health plans, including Medicare, to assess a physician's quality and cost are not always transparent or easy to interpret, which makes it extremely difficult for physicians to improve quality and provide better value. Often the methodologies used to asses a physician's quality and/or cost conflict with the methodologies used for public reporting. Based on the AMA's analysis of available Medicare data, in several instances, physicians deemed to be of similar quality by one methodology were classified as having different levels of quality by other methodology. Additionally, some physicians classified in the highest (or lowest) level of quality by one methodology were not classified as such by the other methodology. The inconsistencies may result in physician frustration and dissatisfaction, and lead to a lack of confidence in the quality programs. Furthermore, it could lead to patients making incorrect assumptions about physician quality when deciding where to seek care.

Price Information in EHI

As stated above, the AMA believes that defining EHI to include various types of price information and then holding physicians and other entities accountable under the information blocking provisions is inappropriate because this pricing information is generally held and controlled by health plans. These plans are not subject to the information blocking provisions and therefore do not have the same incentives to share information. Moreover, given the complexity surrounding specific plans, deductibles, level of coinsurance, and site of service, payment calculations for the future provision of health care to a patient may prove difficult in providing an accurate estimate. Pushing out price information for the sake of pushing out price information without it being meaningful and accurate is worthless and counterproductive.

Request for comment regarding price information (Department of Health and Human Services)

The overall Department seeks comment on the technical, operational, legal, cultural, environmental and other challenges to creating price transparency within health care.

Preamble FR Citation: 84 FR 7513-14 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

Please see the above response to the price information RFI.

Request for comment regarding practices that may implicate the information blocking provision

We request comment regarding our proposals about practices that may implicate the information blocking provision. Specifically, we seek comment on:

- Our proposed approach regarding observational health information and encourage commenters to identify potential practices related to non-observational health information that could raise information blocking concerns.
- The circumstances described and other circumstances that may present an especially high likelihood that a practice will interfere with access, exchange, or use of EHI within the meaning of the information blocking provision.

Preamble FR Citation: 84 FR 7515-21 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

The AMA finds these examples helpful and should provide a useful basis for sub-regulatory guidance. At the same time, some of the examples raise issues that point to needed revisions in both ONC regulatory provisions and agency interpretations.

We are very concerned with the complexity and broad reach resulting from the interaction of the pricing provisions of the proposed rule, in both information blocking practices and exception, with the very expansive definitions of actors and of EHI. Although ONC refers to “rent-seeking and other opportunistic pricing practices,” its definition is not limited to such behaviors and will likely to be very subjective. For example, ONC implies that “value-based pricing”—an approach commonly used in industry—is “opportunistic” and would not be mitigated by any of the proposed exceptions. ONC goes on to emphasize that

> *“[T]he reach of the information blocking provision is not limited to these types of practices. We interpret the definition of information blocking to encompass any fee that materially discourages or otherwise imposes a material impediment to access, exchange, or use of EHI. We use the term “fee” in the broadest possible sense to refer to any present or future obligation to pay money or provide any other thing of value . . . We believe this scope may be broader than necessary to address genuine information blocking concerns and could unnecessarily diminish investment and innovation in interoperable technologies and services. Therefore, . . . we propose to create an exception that, subject to certain conditions, would permit the recovery of costs that are reasonably incurred to provide access, exchange, and use of EHI.”*

It appears that ONC would view any fee as imposing a “material impediment” and therefore requiring use of the exception focused on recovering costs. ONC acknowledges that the definition of any fee as a practice that implicates information blocking “may be broader than necessary to address genuine information blocking concerns and could unnecessarily diminish investment and innovation in interoperable technologies and services”. We agree with ONC on this latter point but are not convinced that simply providing an exception, which is itself very limiting, is a sufficient counter to the issues raised by the provision. In addition, the documentation required by these exceptions could be quite extensive and onerous. **We note that Cures directs HHS to reduce physician burden, not increase it.**

VIII.D Proposed Exceptions to the Information Blocking Provision

§ 171.201 Exception – Preventing harm

To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.

(a) The actor must have a reasonable belief that the practice will directly and substantially reduce the likelihood of harm to a patient or another person arising from—

(1) Corrupt or inaccurate data being recorded or incorporated in a patient's electronic health record;

(2) Misidentification of a patient or patient's electronic health information; or

(3) Disclosure of a patient's electronic health information in circumstances where a licensed health care professional has determined, in the exercise of professional judgment, that the disclosure is reasonably likely to endanger the life or physical safety of the patient or another person, provided that, if required by applicable federal or state law, the patient has been afforded any right of review of that determination.

(b) If the practice implements an organizational policy, the policy must be—

(1) In writing;

(2) Based on relevant clinical, technical, and other appropriate expertise;

(3) Implemented in a consistent and non-discriminatory manner; and

(4) No broader than necessary to mitigate the risk of harm.

(c) If the practice does not implement an organizational policy, an actor must make a finding in each case, based on the particularized facts and circumstances, and based on, as applicable, relevant clinical, technical, and other appropriate expertise, that the practice is necessary and no broader than necessary to mitigate the risk of harm.

Preamble FR Citation: 84 FR 7523-26 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

The AMA is concerned that ONC's expectations for the ability to carve out 42 CFR Part 2 covered data may far exceed current industry capabilities in terms of technology and operational capacity. In particular, carving out such data from notes for exchange and data export will be very challenging. We suggest that the focus on physical harm in the determination by a licensed health care professional is too narrow and should be expanded to include psychological and other forms of non-physical harm. Additionally, the proposed burden of proof is unreasonable and the need to demonstrate that a policy is sufficiently tailored is likely to create a costly compliance burden. **We note that Cures directs HHS to reduce physician burden, not increase it.**

§ 171.202 Exception – Promoting the privacy of electronic health information

To qualify for this exception, each practice by an actor must satisfy at least one of the sub-exceptions in paragraphs (b) through (e) of this section at all relevant times.

(a) Meaning of "individual" in this section. The term "individual" as used in this section means one or more of the following—

(1) An individual as defined by 45 CFR 160.103.

(2) Any other natural person who is the subject of the electronic health information being accessed, exchanged, or used.

(3) A person who legally acts on behalf of a person described in paragraph (a)(1) or (2) of this section, including as a personal representative, in accordance with 45 CFR 164.502(g).

(4) A person who is a legal representative of and can make health care decisions on behalf of any person described in paragraph (a)(1) or (2) of this section.

(5) An executor, administrator or other person having authority to act on behalf of a deceased person described in paragraph (a)(1) or (2) of this section or the individual's estate under State or other law.

(b) Precondition not satisfied. If the actor is required by a state or federal privacy law to satisfy a condition prior to providing access, exchange, or use of electronic health information, the actor may choose not to provide access, exchange, or use of such electronic health information if the precondition has not been satisfied, provided that—

(1) The actor's practice—

(i) Conforms to the actor's organizational policies and procedures that:

~~(A)~~ Are in writing;

~~(B)~~ Specify the criteria to be used by the actor and, as applicable, the steps that the actor will take, in order that the precondition can be satisfied; and

~~(C)~~ Have been implemented, including by taking reasonable steps to ensure that its workforce members and its agents understand and consistently apply the policies and procedures; or

(ii) Has been documented by the actor, on a case-by-case basis, identifying the criteria used by the actor to determine when the precondition would be satisfied, any criteria that were not met, and the reason why the criteria were not met; and

(2) If the precondition relies on the provision of consent or authorization from an individual, the actor:

(i) Did all things reasonably necessary within its control to provide the individual with a meaningful opportunity to provide the consent or authorization; and

(ii) Did not improperly encourage or induce the individual to not provide the consent or authorization.

(3) The actor's practice is—

(i) Tailored to the specific privacy risk or interest being addressed; and

(ii) Implemented in a consistent and non-discriminatory manner.

c) Health IT developer of certified health IT not covered by HIPAA. If the actor is a health IT developer of certified health IT that is not required to comply with the HIPAA Privacy Rule when engaging in a practice that promotes the privacy interests of an individual, the actor may choose not to

§ 171.202 Exception – Promoting the privacy of electronic health information

provide access, exchange, or use of electronic health information provided that the actor's practice—

(1) Complies with applicable state or federal privacy laws;

(2) Implements a process that is described in the actor's organizational privacy policy;

(3) Had previously been meaningfully disclosed to the persons and entities that use the actor's product or service;

(4) Is tailored to the specific privacy risk or interest being addressed; and

(5) Is implemented in a consistent and non-discriminatory manner.

(d) Denial of an individual's request for their electronic protected health information in the circumstances provided in 45 CFR 164.524(a)(1), (2), and (3). If an individual requests their electronic protected health information under 45 CFR 164.502(a)(1)(i) or 45 CFR 164.524, the actor may deny the request in the circumstances provided in 45 CFR 164.524(a)(1), (2), or (3).

(e) Respecting an individual's request not to share information. In circumstances where not required or prohibited by law, an actor may choose not to provide access, exchange, or use of an individual's electronic health information if—

(1) The individual requests that the actor not provide such access, exchange, or use;

(2) Such request is initiated by the individual without any improper encouragement or inducement by the actor;

(3) The actor or its agent documents the request within a reasonable time period; and

(4) The actor's practice is implemented in a consistent and non-discriminatory manner.

Preamble FR Citation: 84 FR 7526-35 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

The AMA is concerned that the requirement that the actor "[d]id all things reasonably necessary within its control to provide the individual with a meaningful opportunity to provide the consent or authorization" is too rigid. If even one possible action was not done, the exception would not apply. Despite the OCR guidance on the HIPAA Right of Access and Apps, physicians and developers will feel a need and obligation for some due diligence. ONC must also be more realistic about the complexities and challenges of separating out 42 CFR Part 2 data from other EHI, especially when the information is contained in clinical notes. There are important overlaps between privacy and security that must be recognized.

Furthermore, we have concern that the proposed exceptions do not sufficiently recognize the kinds of bad actors that are present in the environment. For example, organizations that employ security-related attacks on other organizations and those that may have received authorization to access data but collect more than authorized or use the information in unauthorized ways. It is essential that the exception enables actors to address the range of such security threats, including those posed by state actors.

As discussed above, physicians may have a valid, reasonable reason to restrict the exchange of information. **Yet ONC's interpretation of Cures creates an assumption that any physician who withholds data is**

guilty of information blocking. To counter this assumption and to justify withholding information for any reason, physicians must divert time and resources away from patient care to dissecting incredibly complex exceptions that are riddled with subjective terminology. Once a physician does so (potentially by hiring attorneys or consultants at great expense to the practice), he or she must create new policies and procedures, train staff, and adjust workflows. Furthermore, physicians may need to document the justification for applying those exceptions for every single request of information. The inherent presumption of guilt, complex sub-exceptions, and substantial added burdens of ONC's proposal exceed the scope of Cures' intent. ONC should create policies that identify bad actors without placing considerable burden on the rest of the health care system. Otherwise physicians will be tasked, time and time again, with the chore of documenting decisions that should be left to the physician's best judgement. Or, alternatively, they will just share whatever information they are asked for, regardless of whether the requestor has valid reasons for doing so, and the physician risks penalties for that, too. In either scenario, physicians and patients lose.

By way of example, we highlight ONC's proposed minimum necessary exception and its effect on patient privacy. Prioritizing data quantity over usability presents significant privacy concerns. For example, a directive to exchange all EHI with any requestor for nearly any purpose may force physicians to compromise the "minimum necessary" standard in HIPAA. **The AMA supports maintaining HIPAA's minimum necessary standard, which generally requires physicians to share the minimum amount of information necessary to accomplish the intended purpose of the disclosure.**[23] For instance, we do not support requirements to disclose an entire designated record set to another covered entity. We also do not support a requirement to disclose psychotherapy notes—we note that even patients do not have access rights to their psychotherapy notes. Minimum necessary controls are particularly important given the Administration's clear intent to promote the exchange of information above all else and the emerging capability of technology to extract bulk patient data out of an EHR.

Confusion about HIPAA's minimum necessary standard versus ONC's EHI-based information blocking requirements will lead to oversharing of patient data. Some clinicians may find it easier (and less worrisome from an enforcement perspective) to simply disclose everything they have. Additionally, the Meaningful Use Program demonstrated that when requirements to exchange data exist, but lack minimum necessary standards, health care organizations will send everything to ensure they comply with the requirement to exchange.[24,25,26] The receiving physician is then saddled with the enormous burden of reviewing all the information to glean what is clinically relevant. Furthermore, while we appreciate ONC's inclusion of a minimum necessary sub-exception, the efforts required to assert the sub-exception are excessive. Attempting to determine how much information to divulge so as not to violate HIPAA and face OCR enforcement or ONC's information blocking rules (evoking OIG enforcement) amounts to significant cognitive burden. Those who do make such determinations are required to create new policy and procedures[27] and navigate multiple exceptions or sub-exceptions. Both scenarios are a result of increased regulatory complexity that contradicts Congress' intent to reduce physician burden.

[23] 45 CFR §164.502(b).

[24] Dr. David Barbe, President-elect American Medical Association, *EHR Innovation and Problem-Solving: Physician Perspective*, 2016, available at: https://www.healthit.gov/sites/default/files/David_Barbe-Innovation_&_Problem-Solving.pdf.

[25] Reisman, Miriam, *EHRs: The Challenge of Making Electronic Data Usable and Interoperable*, P & T : a peer-reviewed journal for formulary management vol. 42,9 (2017): 572-575, available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5565131/.

[26] EHR Intelligence, *GAO: Lack of data standards foils EHR interoperability, HIE*, 2014, available at: https://ehrintelligence.com/news/gao-lack-of-data-standards-foils-ehr-interoperability-hie.

[27] ONC proposes that for an actor to qualify for an information blocking sub-exception, the actor's privacy policies and procedures would need to identify criteria for making a "minimum necessary" determination for both routine and non-routine disclosures and requests, including identifying the circumstances under which disclosing the entire medical record is reasonably necessary. HIPAA only requires policy determinations be established for non-routine disclosures.

Exploiting the link between minimum necessary and information blocking requirements may also lead to "bullying." For example, physicians already have established processes to determine what constitutes the minimally necessary amount of information to process claims. This balances adjudication needs with clinical judgment and patient privacy. As proposed, EHI and information blocking requirements may empower payers to demand more information than is needed. Patients trust physicians to safeguard access to their most personal information, only sharing it for appropriate purposes and with their consent. We highlight that, while ONC repeatedly promotes payers' access to data, Congress refrained from mentioning payers in Cures' information blocking provision. **ONC seems to conflate the interests of payers with clinicians' need to access, exchange, or use health information.** Further, payers are not subject to information blocking requirements and are therefore emboldened to use (and withhold) information as they see fit. Unfortunately, under ONC's proposal, a physician who denies a payer's request for EHI—regardless of whether the request is fully warranted—may implicate the physician in information blocking.

To address concerns not only with minimum necessary standards, but the misguided approach to presumption of guilt around information blocking, **ONC should clarify that a physician exercising his or her best judgement when providing information to a requestor will not be considered an information blocker. ONC should also remove onerous requirements for physician to document their decision-making associated with qualifying for information blocking exceptions or sub-exceptions.**

§ 171.203 Exception – Promoting the security of electronic health information

To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.

(a) The practice must be directly related to safeguarding the confidentiality, integrity, and availability of electronic health information.

(b) The practice must be tailored to the specific security risk being addressed.

(c) The practice must be implemented in a consistent and non-discriminatory manner.

(d) If the practice implements an organizational security policy, the policy must—

(1) Be in writing;

(2) Have been prepared on the basis of, and directly respond to, security risks identified and assessed by or on behalf of the actor;

(3) Align with one or more applicable consensus-based standards or best practice guidance; and

(4) Provide objective timeframes and other parameters for identifying, responding to, and addressing security incidents.

(e) If the practice does not implement an organizational security policy, the actor must have made a determination in each case, based on the particularized facts and circumstances, that:

(1) The practice is necessary to mitigate the security risk to the electronic health information; and

(2) There are no reasonable and appropriate alternatives to the practice that address the security risk that are less likely to interfere with, prevent, or materially discourage access, exchange or use of electronic health information.

Preamble FR Citation: 84 FR 7535-38 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

The AMA is concerned with the burden on physicians to perform analyses of their policies and practices against complex and incompletely defined terms—especially with the requirement to meet “all requirements at all times”.

We note that this exception has a provision for cases where there is no written policy. In practice, it seems most likely that the absence of a policy means that one is dealing with an unexpected and evolving situation as best one can (e.g., a sustained and sophisticated attack). The exception calls for a determination that not only that the practice is necessary, but also that effectively there is no other way of having protected your security that might have been less likely to interfere with information access. In our view, such a requirement is asking too much of those dealing with urgent threats, often after hours and under considerable uncertainty. **We suggest that ONC create a further “safety valve” for short-lived actions that are taken in good faith while a situation is being evaluated and understood. We believe this is a core need for small medical practices with limited resources.**

We ask that ONC clarify that proactive and preventive security-focused activities are permitted so long as they meet the applicable criteria for security-related practices in this exception.

ONC should confirm that an organization can use security policies that exceed what is required by law or regulation based on their assessment of the threat environment, without violating this exception. ONC should recognize the valid need to allow for due diligence as distinct from simply delaying access and such due diligence should not need the security exception to avoid implicating or being judged as engaged in information blocking. The need for vetting of external locations of exchange includes but is not limited to apps. (e.g., networks).

AMA research has shown that 85 percent of physicians believe it is very important to share electronic health information—they just want to do it safely and within their means.[28] Unfortunately, cyberattacks are inevitable and increasing, leading numerous agencies across the federal government to recognize cybersecurity as a patient safety issue.[29] In fact, the AMA's research revealed that eight in 10 physicians have experienced some form of attack and only 20 percent of small practices have internal security officers despite the fact that 71 percent of ransomware attacks targeted small businesses in 2018.[30, 31] Even if a physician's office houses relatively few health care records, it may be connected to other health systems with significantly more data.

These statistics contextualize the security environment in which physicians will need to navigate information blocking requirements. Yet, **ONC's proposals will require physicians to adjust their systems to permit "access", "exchange", and "use" of EHI in new ways—resulting in a series of "trial and error" scenarios and forcing EHR vendors and physicians to guess at what should be accessed or used and from whom.** This could result in exposing multiple entry points to cyber attackers seeking to exploit vulnerabilities, exposing more data than ever before given the amount of information ONC is proposing that actors share. These adversaries will target the weakest link in the chain, which may be a physician office or legacy technologies.

ONC's proposals will enable unprecedented electronic access and modification to medical records. Professional societies representing practice administrators, health system chief information officers, and security professionals are already expressing apprehension.[32,33,34] Concerningly, they all sound alarms that EHRs will not sufficiently protect the "use" of EHI as envisioned by ONC. ONC defines *use* in § 171.102 as

[28] AMA, *Patient Safety: The Importance of Cybersecurity in Health Care*, 2018, available at: https://www.ama-assn.org/system/files/2018-10/cybersecurity-health-care-infographic.pdf.

[29] U.S. Food and Drug Administration, FDA News Release, 2018, available at: https://www.fda.gov/news-events/press-announcements/fda-and-dhs-increase-coordination-responses-medical-device-cybersecurity-threats-under-new.

[30] AMA, *Medical Cybersecurity: A Patient Safety Issue*, 2017, available at: https://www.ama-assn.org/delivering-care/patient-support-advocacy/medical-cybersecurity-patient-safety-issue.

[31] Health IT Security, *71% of Ransomware Attacks Targeted Small Businesses in 2018*, March 2019, available at: https://healthitsecurity.com/news/amp/71-of-ransomware-attacks-targeted-small-businesses-in-2018.

[32] Health IT Security, *As ONC Considers Info Blocking, IoT, Medical Device Guidance Needed*, April 2019, available at: https://healthitsecurity.com/news/as-onc-considers-info-blocking-iot-medical-device-guidance-needed?eid=CXTEL000000154738&elqCampaignId=9253&elqTrackId=151c5e0bac4b4df6b2155ef6a9ffce20&elq=9d083122ab044763baa6817a857a7474&elqaid=9715&elqat=1&elqCampaignId=9253.

[33] Fierce Healthcare, *Complying with information blocking rule will be a challenge without standardized APIs: HIMSS*, March 2019, available at: https://www.fiercehealthcare.com/tech/complying-information-blocking-rule-will-be-a-challenge-without-standardized-apis-himss.

[34] Health IT Security, *ONC Information Blocking Rule Raises Privacy and Security Concerns*, March 2019, available at: https://healthitsecurity.com/news/onc-information-blocking-rule-raises-privacy-and-security-concerns?eid=CXTEL000000154738&elqCampaignId=8938&elqTrackId=7b46f9fd83434ed99efae92be850fefd&elq=89d147ceb6e246fd99eed1ba66e334b3&elqaid=9402&elqat=1&elqCampaignId=8938.

the ability of health IT or a user of health IT to access relevant electronic health information; to comprehend the structure, content, and meaning of the information; and to read, write, modify, manipulate, or apply the information to accomplish a desired outcome or to achieve a desired purpose.

There are major implications for EHI *use* as proposed by ONC. For one, **using EHI would allow an actor (e.g., a consumer-facing app developer) the ability to *read, write,* and *modify* a patient's medical record—including financial, demographic, genetic, protected SUD or mental health, and family information, in an EHR. This is a staggering shift from current EHR capabilities.** Not only are APIs and ONC's proposed API requirements woefully insufficient to protect bi-direction exchange of data, but security experts who participate as HHS advisors have themselves highlighted the need for major security and privacy controls to comply ONC's information blocking proposals.

Before enacting the information blocking rule, ONC should first consider selecting or establishing a security controls framework for interoperability and data sharing processes that would support the trusted environments necessary "to build confidence in payers, providers, and patients."[35,36]

Furthermore, Christopher Wray, the Director of the U.S. Federal Bureau of Investigation (FBI), announced in March 2019 that, "Today's cyberthreat is bigger than any one government agency—in fact it's bigger than the government itself," and that "the scope, breadth, depth, sophistication and diversity of the threat we face now is unlike anything we've had in our lifetimes."[37] These circumstances raise numerous questions:

- **Has ONC established a security controls framework for interoperability and data sharing?**
- **How will ONC, a single government agency, ensure EHI access, exchange, and use does not compromise the personal health information of U.S. citizens?**
- **What is ONC's plan to ensure that thousands of apps properly authenticate for EHI use?**
- **What is ONC's plan for protecting the multiple access points and attack surfaces that will be necessary to facilitate EHI use?**
- **How is ONC going to ensure EHR vendors develop and test to security industry protective measures, prescribed standards, and security protocols?**

The federal government needs to empower physicians to actively manage their security posture, not hinder them**.** We seek clarity from ONC as to whether it expects physicians to use information blocking exceptions and documentation as "protection" from these risks.

[35] Id.

[36] CynergisTek is represented on The Healthcare and Public Health Sector Coordinating Council (HSCC).

[37] Healthcare IT News, *RSA 2019: FBI Director Christopher Wray says 'today's cybersecurity threat is bigger than government itself'*, March 2019, available at: https://www.healthcareitnews.com/news/rsa-2019-fbi-director-christopher-wray-says-today%E2%80%99s-cybersecurity-threat-bigger-government?mkt_tok=eyJpIjoiTWpjd05HRmtZV0V3WW1OaiIsInQiOiJYN2Q0dVhtQUxHRytncTl1NlZSWXdlekZCSWpMU3hoUmFqZlwvdzBacTBZTjBrR1hWZmlRYWlkc1VpV0RhdE9xWUc5VjF0TDFZNGo2TnV6VG1aZlRndGd6SXRoTFFVWTFUV3Zqdm5YUVNhWUhsSm9ua2tHV1wvTWEwY0hWWHBLN1N1In0%3D.

§ 171.204 Exception – Recovering costs reasonably incurred

To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.

(a) Types of costs to which this exception applies. This exception is limited to the actor's costs reasonably incurred to provide access, exchange, or use of electronic health information.

(b) Method for recovering costs. The method by which the actor recovers its costs—

(1) Must be based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests;

(2) Must be reasonably related to the actor's costs of providing the type of access, exchange, or use to, or at the request of, the person or entity to whom the fee is charged;

(3) Must be reasonably allocated among all customers to whom the technology or service is supplied, or for whom the technology is supported;

(4) Must not be based in any part on whether the requestor or other person is a competitor, potential competitor, or will be using the electronic health information in a way that facilitates competition with the actor; and

(5) Must not be based on the sales, profit, revenue, or other value that the requestor or other persons derive or may derive from the access to, exchange of, or use of electronic health information, including the secondary use of such information, that exceeds the actor's reasonable costs for providing access, exchange, or use of electronic health information.

(c) Costs specifically excluded. This exception does not apply to—

(1) Costs that the actor incurred due to the health IT being designed or implemented in non-standard ways that unnecessarily increase the complexity, difficulty or burden of accessing, exchanging, or using electronic health information;

(2) Costs associated with intangible assets (including depreciation or loss of value), other than the actual development or acquisition costs of such assets;

(3) Opportunity costs, except for the reasonable forward-looking cost of capital;

(4) A fee prohibited by 45 CFR 164.524(c)(4);

(5) A fee based in any part on the electronic access by an individual or their personal representative, agent, or designee to the individual's electronic health information;

(6) A fee to perform an export of electronic health information via the capability of health IT certified to § 170.315(b)(10) of this subchapter for the purposes of switching health IT or to provide patients their electronic health information; or

(7) A fee to export or convert data from an EHR technology, unless such fee was agreed to in writing at the time the technology was acquired.

(d) Compliance with the Conditions of Certification.

§ 171.204 Exception – Recovering costs reasonably incurred

(1) Notwithstanding any other provision of this exception, if the actor is a health IT developer subject to the Conditions of Certification in § 170.402(a)(4) or § 170.404 of this subchapter, the actor must comply with all requirements of such conditions for all practices and at all relevant times.

(2) If the actor is an API Data Provider, the actor is only permitted to charge the same fees that an API Technology Supplier is permitted to charge to recover costs consistent with the permitted fees specified in the Condition of Certification in § 170.404 of this subchapter.

Preamble FR Citation: 84 FR 7538-41 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

The AMA agrees that ONC should prioritize exchange, access, and use of "observational health information" (i.e., EHI that is created or maintained during the practice of medicine or the delivery of health care services to patients). In addition, we believe that ONC should also prioritize certain purposes or use cases for data exchange/access/use, specifically, the HIPAA categories of treatment, payment, and operations, relative to access (other than that needed to support a patient's HIPAA right of access) that is intended to serve primarily clinical care objectives of the party seeking data.

§ 171.205 Exception – Responding to requests that are infeasible

To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.

(a) Request is infeasible.

(1) The actor must demonstrate, in accordance with paragraph (a)(2) of this section, that complying with the request in the manner requested would impose a substantial burden on the actor that is unreasonable under the circumstances, taking into consideration—

(i) The type of electronic health information and the purposes for which it may be needed;

(ii) The cost to the actor of complying with the request in the manner requested;

(iii) The financial, technical, and other resources available to the actor;

(iv) Whether the actor provides comparable access, exchange, or use to itself or to its customers, suppliers, partners, and other persons with whom it has a business relationship;

(v) Whether the actor owns or has control over a predominant technology, platform, health information exchange, or health information network through which electronic health information is accessed or exchanged;

(vi) Whether the actor maintains electronic protected health information on behalf of a covered entity, as defined in 45 CFR 160.103, or maintains electronic health information on behalf of the requestor or another person whose access, exchange, or use of electronic health information will be enabled or facilitated by the actor's compliance with the request;

(vii) Whether the requestor and other relevant persons can reasonably access, exchange, or use the electronic health information from other sources or through other means; and

§ 171.205 Exception – Responding to requests that are infeasible

(viii) The additional cost and burden to the requestor and other relevant persons of relying on alternative means of access, exchange, or use.

(2) The following circumstances do not constitute a burden to the actor for purposes of this exception and shall not be considered in determining whether the actor has demonstrated that complying with a request would have been infeasible.

(i) Providing the requested access, exchange, or use in the manner requested would have facilitated competition with the actor.

(ii) Providing the requested access, exchange, or use in the manner requested would have prevented the actor from charging a fee.

(b) Responding to requests. The actor must timely respond to all requests relating to access, exchange, or use of electronic health information, including but not limited to requests to establish connections and to provide interoperability elements.

(c) Written explanation. The actor must provide the requestor with a detailed written explanation of the reasons why the actor cannot accommodate the request.

(d) Provision of a reasonable alternative. The actor must work with the requestor in a timely manner to identify and provide a reasonable alternative means of accessing, exchanging, or using the electronic health information.

Preamble FR Citation: 84 FR 7542-44 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

The AMA is concerned that this exception is too vague. This vagueness will create uncertainty as to whether claiming this exception will ultimately be validated by regulators and therefore lessen the benefit of this important exception.

The AMA recommends ONC include requests for data that would use non-standard implementation specifications be refused as “infeasible. Furthermore, actors should be able to focus on specific use cases and refuse requests to expand access, exchange, or use to support additional use cases as “infeasible.” At the same time, we believe that there should be a floor of the minimum set of use cases with associated interoperability standards that must be supported by a specific type of actor; perhaps the TEFCA provides a basis for such a floor.

We ask ONC to confirm that infeasibility could include not having the technical capability in production to meet a request (e.g., not having APIs or other technical means to support a specific type of exchange, access, or use, for example to enable write access to the EHR), when the cost of acquiring such capabilities are excessive and could reduce the ability to meet other project plans and customer commitments.

We ask ONC to consider whether a request can be deemed infeasible if there is another widely accepted alternative for performing the same or comparable action.

We do not believe that this exception should need to be invoked, or information blocking implicated, if, per the regulatory language, the actor works “with the requestor in a timely manner to identify and provide a reasonable alternative means of accessing, exchanging, or using the electronic health information".

We ask ONC to confirm lack of backwards compatibility of standards could be a basis for invoking this exception, for example if ONC finalizes its proposal to allow both FHIR DSTU 2 and FHIR Release 4.

We encourage ONC to establish a more unified interoperable infrastructure so that patients can safely and securely access their medical records using the app of their choice. Many of these apps are already being developed to support the USCDI data elements. Coordinating efforts around the USCDI and APIs will provide more value for patients than a bulk dump of unstructured data. Apps should be able to get data from an EHR through known protocols and standards—providing an easy-to-use and easy-to-understand cohesive data set. Policy efforts should promote technical requirements to deliver a defined concept of EHI to patients in a computable format so that their data can be used once made available. It is likely that an EHR will have multiple APIs, each connecting to a different service. We expect EHR vendors will eventually establish an orchestration of secure API services to facilitate access and use to the complete medical record. **ONC should encourage this approach by promoting the USCDI as a logical interoperability building block.**

Alignment between ONC's information blocking, EHI, and USCDI proposals could happen in several ways. The AMA is recommending two potential paths:

- ONC could constrain its definition of EHI to just the data elements represented by the USCDI for specified actors. Information blocking requirements would be subject to newly-scoped access, use, and exchange of the USCDI. Patients would retain their rights to request their designated record set as outlined by HIPAA (the Director of the HHS Office of Civil Rights has already noted publicly that patient access enforcement will increase this year). EHI export could be scoped to focus on ePHI as outlined by HIPAA. Additional data classes (e.g., payment and cost information) would propagate through the USCDI expansion process with support from the ISA and SVAP.

- Alternatively, ONC could retain its EHI definition, rescope the terms "access", "use", and "exchange", and include additional information blocking exceptions. ONC could establish an exception for actors only able to make the USCDI available. This exception should be concise, clear, implementable, and refrain from burdensome policy and procedure requirements. **This could also be accomplished by modifying the proposed "Infeasibility of Request" exception.** We encourage ONC to clarify that actors that do not comply with the request for access, exchange, or use of EHI, but that do comply to the best of their ability with requests for access, exchange, or use of the USCDI be able to claim this exception. Also, ONC should clarify that an actor could claim an exception for responding in "good faith" to requests beyond the USCDI.

§ 171.206 Exception – Licensing of interoperability elements on reasonable and non-discriminatory terms

To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.

(a) Responding to requests. Upon receiving a request to license or use interoperability elements, the actor must respond to the requestor within 10 business days from receipt of the request by:

(1) Negotiating with the requestor in a reasonable and non-discriminatory fashion to identify the interoperability elements that are needed; and

(2) Offering an appropriate license with reasonable and non-discriminatory terms.

(b) Reasonable and non-discriminatory terms. The actor must license the interoperability elements described in paragraph (a) of this section on terms that are reasonable and non-discriminatory.

§ 171.206 Exception – Licensing of interoperability elements on reasonable and non-discriminatory terms

(1) Scope of rights. The license must provide all rights necessary to access and use the interoperability elements for the following purposes, as applicable.

(i) Developing products or services that are interoperable with the actor's health IT, health IT under the actor's control, or any third party who currently uses the actor's interoperability elements to interoperate with the actor's health IT or health IT under the actor's control.

(ii) Marketing, offering, and distributing the interoperable products and/or services to potential customers and users.

(iii) Enabling the use of the interoperable products or services in production environments, including accessing and enabling the exchange and use of electronic health information.

(2) Reasonable royalty. If the actor charges a royalty for the use of the interoperability elements described in paragraph (a) of this section, the royalty must be reasonable and comply with the following requirements.

(i) The royalty must be non-discriminatory, consistent with paragraph (b)(3) of this section.

(ii) The royalty must be based solely on the independent value of the actor's technology to the licensee's products, not on any strategic value stemming from the actor's control over essential means of accessing, exchanging, or using electronic health information.

(iii) If the actor has licensed the interoperability element through a standards development organization in accordance with such organization's policies regarding the licensing of standards-essential technologies on reasonable and non-discriminatory terms, the actor may charge a royalty that is consistent with such policies.

(3) Non-discriminatory terms. The terms (including royalty terms) on which the actor licenses and otherwise provides the interoperability elements must be non-discriminatory and comply with the following requirements.

(i) The terms must be based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests.

(ii) The terms must not be based in any part on—

(A) Whether the requestor or other person is a competitor, potential competitor, or will be using electronic health information obtained via the interoperability elements in a way that facilitates competition with the actor; or

(B) The revenue or other value the requestor may derive from access, exchange, or use of electronic health information obtained via the interoperability elements, including the secondary use of such electronic health information.

(4) Collateral terms. The actor must not require the licensee or its agents or contractors to do, or to agree to do, any of the following.

(i) Not compete with the actor in any product, service, or market.

(ii) Deal exclusively with the actor in any product, service, or market.

(iii) Obtain additional licenses, products, or services that are not related to or can be unbundled from the requested interoperability elements.

§ 171.206 Exception – Licensing of interoperability elements on reasonable and non-discriminatory terms

(iv) License, grant, assign, or transfer to the actor any intellectual property of the licensee.

(v) Pay a fee of any kind whatsoever, except as described in paragraph (b)(2) of this section, unless the practice meets the requirements of the exception in § 171.204.

(5) Non-disclosure agreement. The actor may require a reasonable non-disclosure agreement that is no broader than necessary to prevent unauthorized disclosure of the actor's trade secrets, provided—

(i) The agreement states with particularity all information the actor claims as trade secrets; and

(ii) Such information meets the definition of a trade secret under applicable law.

(c) Additional requirements relating to the provision of interoperability elements. The actor must not engage in any practice that has any of the following purposes or effects.

(1) Impeding the efficient use of the interoperability elements to access, exchange, or use electronic health information for any permissible purpose.

(2) Impeding the efficient development, distribution, deployment, or use of an interoperable product or service for which there is actual or potential demand.

(3) Degrading the performance or interoperability of the licensee’s products or services, unless necessary to improve the actor’s technology and after affording the licensee a reasonable opportunity to update its technology to maintain interoperability.

(d) Compliance with conditions of certification. Notwithstanding any other provision of this exception, if the actor is a health IT developer subject to the conditions of certification in §§ 170.402, 170.403, or 170.404 of this subchapter, the actor must comply with all requirements of such conditions for all practices and at all relevant times.

Preamble FR Citation: 84 FR 7544-50 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

The AMA seeks clarification of the intended scope of this exception. Is the intent to make this exception available for licensing of Interoperability Elements only? The AMA believes ONC’s intent is to establish the exception as one of seven exceptions to the information blocking provision.

The AMA has the following technical amendments to the exception relating to the licensing on reasonable and nondiscriminatory (RAND) terms. Please also see the below line edits to the exception.

Responding to Requests

The AMA is supportive of the concept of requiring licensors to respond to requests within 10 business days; however, this 10-day response requirement should be for an initial request and cover the actions of offering the license only. The AMA is supportive of two separate timeframes for (1) Negotiating with the requestor and (2) offering the license. Alternatively, ONC may want to considering taking the negotiation timeframe out of the 5-15 business day window altogether. The AMA also believes that any limitations on the amount of time for acceptance of an initial offer or counteroffers, or an allowable number of counteroffers in negotiations would potentially be problematic. ONC should allow for parties to freely negotiate terms without dictating arbitrary limits.

Reasonable and Non-Discriminatory Terms
The license on reasonable and nondiscriminatory terms should match the purpose of the information blocking provision to enable the Access, Exchange, and Use of EHI. Any more specific requirements may read as inappropriate mandates. Alternatively, ONC could leave in proposed subparts (b)(1)(i), (ii) and (iii) with explicit language stating that these subparts are examples and not a limiting mandate.

Additionally, the "independent value" of an actor's technology is vague. Instead, the value should be based on objective and verifiable criteria similar to the method in recovering reasonably incurred costs.

Collateral Terms
ONC must recognize that situations exist where licensors do not have the ability to lawfully confer rights or licenses to information or products without the agreement of a third party. Thus, "except as required by law" should be added to clarify that the expectation is not for an actor to obtain such rights on behalf of the requestor.

§ 171.206 Exception—Licensing of interoperability elements on reasonable and non-discriminatory terms.

To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.
a. *Responding to requests.* Upon receiving a request to license or use interoperability elements and provided that the actor is authorized to license or use such interoperability element, the actor must respond to the requestor within 10 business days from receipt of the initial request by:

(1) ~~Negotiating~~ Offering and seeking to negotiate a license with the requestor and negotiating such a license (pursuant to the requestor's willingness to negotiate) in a reasonable and non-discriminatory fashion to identify the interoperability elements that are needed; and

(2) Offering an appropriate license with reasonable and non-discriminatory terms consistent with the actor's customary licensing models and programs.

b. *Reasonable and non-discriminatory terms.* The actor must license the interoperability elements described in paragraph (a) of this section on terms that are reasonable and non-discriminatory.

(1) *Scope of rights.* The license must provide all rights necessary to access and use the interoperability elements to enable the ~~for the following purposes, as applicable.~~

~~(i) Developing products or services that are interoperable with the actor's health IT, health IT under the actor's control, or any third party who currently uses the actor's interoperability elements to interoperate with the actor's health IT or health IT under the actor's control.~~

~~(ii) Marketing, offering, and distributing the interoperable products and/or services to potential customers and users.~~

~~(iii) Enabling the use of the interoperable products or services in production environments, including and enabling the~~, access, exchange, and use of electronic health information.

(2) *Reasonable royalty.* If the actor charges a royalty for the use of the interoperability elements described in paragraph (a) of this section, the royalty must be reasonable and comply with the following requirements.

(i) The royalty must be non- discriminatory, consistent with paragraph (b)(3) of this section.

(ii) The royalty must be based solely on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests and ~~the independent value of the actor’s technology to the licensee’s products,~~ not on any strategic value stemming from the actor’s control over essential means of accessing, exchanging, or using electronic health

* * * * *

(4) *Collateral terms.* The actor must not require the licensee or its agents or contractors to do, or to agree to do, any of the following.

(i) Not compete with the actor in any product, service, or market.

(ii)Deal exclusively with the actor in any product, service, or market.

(iii)Except as required by law, o~~O~~btain additional licenses, products, or services that are not related to or can be unbundled from the requested interoperability elements,

(iv) License, grant, assign, or transfer to the actor any intellectual property of the licensee.

(v) Pay a fee of any kind whatsoever, except as described in paragraph (b)(2) of this section, unless the practice meets the requirements of the exception in § 171.204.

§ 171.207 Exception – Maintaining and improving health IT performance

To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.

(a) Maintenance and improvements to health IT. An actor may make health IT under its control temporarily unavailable in order to perform maintenance or improvements to the health IT, provided that the actor's practice is—

(1) For a period of time no longer than necessary to achieve the maintenance or improvements for which the health IT was made unavailable;

(2) Implemented in a consistent and non-discriminatory manner; and

(3) If the unavailability is initiated by a health IT developer of certified health IT, HIE, or HIN, agreed to by the individual or entity to whom the health IT developer of certified health IT, HIE, or HIN supplied the health IT.

(b) Practices that prevent harm. If the unavailability of health IT for maintenance or improvements is initiated by an actor in response to a risk of harm to a patient or another person, the actor does not need to satisfy the requirements of this section, but must comply with all requirements of § 171.201 at all relevant times to qualify for an exception.

(c) Security-related practices. If the unavailability of health IT for maintenance or improvements is initiated by an actor in response to a security risk to electronic health information, the actor does not need to satisfy the requirements of this section, but must comply with all requirements of § 171.203 at all relevant times to qualify for an exception.

Preamble FR Citation: 84 FR 7550-52 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

The AMA asks that ONC recognize it is unlikely that physicians would make a system unavailable as part of deliberate information blocking and we question whether such downtime should be considered a practice that implicates information blocking. Physicians have strong incentives to keep systems up and to respond quickly to unplanned outages. We recognize that system unavailability due to prevention of harm or security risks would fall under those exceptions and not this one. At the same time, subjecting urgent system downtime needs to the far-reaching requirements associated with any of these exceptions seems unwarranted.

The language in this exception (preamble and regulation) is not sufficiently clear. For example, what if only one part of a system goes down, such as the gateway for inbound queries?

VIII.F Disincentives for Health Care Providers – Request for Information

Request for information on disincentives for health care providers

We request information on disincentives or if modifying disincentives already available under existing HHS programs and regulations would provide for more effective deterrents to information blocking. We also seek information on the implementation of section 3022(d)(4) of the PHSA, which provides that in carrying out section 3022(d) of the PHSA, the Secretary shall, to the extent possible, not duplicate penalty structures that would otherwise apply with respect to information blocking and the type of individual or entity involved as of the day before December 13, 2016 – enactment of the Cures Act.

Preamble FR Citation: 84 FR 7553 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

The AMA does not support or see a need for any additional penalties or disincentives on providers beyond what is currently in place. In addition to ONC's information blocking requirement, there are already three "levers" to incentivize physicians share and provide access to EHI.

For example, HIPAA requires providers to provide patients access to their designated record set. This includes providing individuals the right to inspect or obtain a copy, or both, of the ePHI, as well as to direct the covered entity to transmit a copy to a designated person or entity of the individual's choice. Providers could face enforcement actions and penalties with monetary fines in the hundreds of thousands, if not millions, for failing to comply with HIPAA regulation. Furthermore, the Office of Civil Rights (OCR) has expressed a desire to increase HIPAA enforcement on providers.

Additionally, to prevent actions that block the exchange of health information, the Medicare Access and CHIP Reauthorization Act of 2015 (MACRA) and the Quality Payment Program (QPP) requires eligible professionals (EP), eligible hospitals (EH) and critical access hospitals (CAH) that participate in both the Medicare and Medicaid Promoting Interoperability (PI) Programs to show that they have not knowingly and willfully limited or restricted the compatibility or interoperability of their certified electronic health record technology (CEHRT). EPs, EHs, and CAHs are required to show that they are meeting this requirement by attesting to three statements about how they implement and use CEHRT. Together, these three statements are referred to as the "Prevention of Information Blocking Attestation." Failing to attest to these statements will result in the EP, EH, or CAH scoring a 0 in PI—resulting in CMS reimbursement penalties. The Centers for Medicare and Medicaid Services (CMS) has also proposed publicly listing the names of EPs, EHs, and CAHs that attest "no".

Lastly, EPs, EHs, and CAHs participating in PI Programs, unless an exclusion is claimed, must submit collected data on four objectives and performance data for certain measures from each of the four objectives' measures. As the program's name entails, the objectives and measures are focused on promoting interoperability. Failing to submit data on the objectives, or performing poorly on the measures, will jeopardize the EPs, EHs, and CAHs, success in the PI Program—resulting in CMS reimbursement penalties.

Therefore, ONC should not create any new disincentives, modify any existing disincentives, or apply any other existing disincentives. Overall, ONC's and OIG's should have a general enforcement approach to encourage consistent compliance with the information blocking provisions rather than punishment. Prior to taking any action against health care providers for violating the information blocking provisions, the first priority should be to work with the health care provider through a corrective action and educational process to remedy the issue.

Section IX – Registries Request for Information

Health IT Solutions Aiding in Bidirectional Exchange with Registries

We believe it is appropriate to explore multiple approaches to advancing health IT interoperability for bidirectional exchange with registries in order to mitigate risks based on factors like feasibility and readiness, potential unintended burden on health care providers, and the need to focus on priority clinical use cases. ONC is therefore seeking information on how health IT solutions and the proposals throughout this rule can aid bidirectional exchange with registries for a wide range public health, quality reporting, and clinical quality improvement initiatives.

We also welcome any other comments stakeholders may have on implementation of the registries provisions under § 4005 of the Cures Act.

Preamble FR Citation: 84 FR 7553-54 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

The AMA encourages ONC to move to a uniform standard for bidirectional exchange between registries and EHRs. Lack of standardization across electronic infrastructure on the data element, definition, and value set level has made implementation of health information technology within registries difficult. FHIR is a superior standard to QRDA and should assist with interoperability. However, USCDI was not developed with an eye towards public health or registry reporting and this needs to be kept in mind as a use case for future development of the USCDI. Having this work originate in a standards development organization would help alleviate this problem.

To further improve interoperability, particularly in the registry space, we encourage ONC and CMS to work with the PCPI. The PCPI for the last several years has been spearheading, in-conjunction with Duke's Clinical Research Institute the "Improving Healthcare Data Interoperability" project, a consensus process, to integrate 23 data elements based on information collected from 38 registries to develop a list of CDEs and associated value sets to be systematically implemented across registries and other source data systems. The goal is to promote semantic interoperability and improve data liquidity in the U.S. health care system.

There is also a need for education and support for registries and public health to implement FHIR—ONC-based support and education are critical in this area for registries to be able to utilize FHIR in a meaningful way.

ONC also needs to monitor EHR vendors for data blocking with registries. Many EHR vendors make registry connectivity cost-prohibitive or put up road blocks for registries to connect to EHRs. Often, we hear it is due to EHR vendors trying to push physicians to utilize the EHR's registry or quality products. However, the products offered by EHR vendors do not always meet the needs of clinicians, particularly specialists and lacks in providing meaningful data feedback, support relevant quality measures and outcome measurement.

Opportunities to Improve Patient Matching
We seek comment on additional opportunities that may exist in the patient matching space and ways that ONC can lead and contribute to coordination efforts with respect to patient matching. ONC is particularly interested in ways that patient matching can facilitate improved patient safety, better care coordination, and advanced interoperability.
Preamble FR Citation: 84 FR 7554-55 **Specific questions in preamble?** *Yes*
Regulatory Impact Analysis: NA

Public Comment Field:

The absence of a consistent approach to accurately identifying patients has resulted in significant costs to the health care system. Patient identification errors often begin during the registration process and can initiate a cascade of errors, including wrong site surgery, delayed or lost diagnoses, and wrong patient orders. As data exchange increases beyond traditional medicine, patient identification and data matching errors will become exponentially more problematic and dangerous. Precision medicine and disease research will continue to be hindered if records are incomplete or duplicative. Accurately identifying patients and matching them to their data is essential to coordination of care and is a requirement for health system transformation and the continuation of our substantial progress towards nationwide interoperability. The AMA shares the goals of CMS and ONC in increasing patient matching to improve patient safety, to better coordinate care, and to advance interoperability.

The above-referenced Sequoia Project document addresses this issue in detail, including, notably, a maturity model for intra-organizational and cross-organizational processes to enhance patient matching accuracy, including rigorous information governance. Overall, the biggest opportunity to immediately enhance matching rates is standardized formats for demographic data among data sharing participants. Additional data elements to improve patient matching efforts may include: Maiden Name, Multiple Birth Indicator, Birth Order, Telephone Number types, and Email Address(es). We also highlight the importance of consistently defined and used format constraints.

Data Collection Standards

Proper and consensus-drive data collection standards may improve the quality of health data that is captured and stored. As with any standards development, having consistent and clear terminology facilitates electronic data collection at the point of care; retrieval of relevant data, information, and knowledge; and data reuse for multiple purposes.

Beyond data collection standards, patient matching software and algorithms may increase the likelihood of accurate data capture. Before any technology is required, any technology should be properly validated with proper indicators. Moreover, to improve data collection, ONC and CMS could create educational and training materials for all levels of administrative staff. This may include incorporating the usefulness of data for detecting and addressing health care needs into the training of health professionals, administrative staff, and hospital and health plan leadership. Despite differences among health care settings, standardizing specific components of data collection through education within each organization will facilitate staff training processes.

Minimum Set of Elements

Important data elements that should be considered as a minimum set of elements that should be collected and exchanged are first name, last name, date of birth, sex, and either zip code (first 5) or phone number. The Sequoia Project conducted a case study analyzing different identity traits for completeness (the percentage of the combined traits that had all the data present in the patients' records) and uniqueness (percentage of matches that resulted in a unique match).[38] The combination of the above identity traits allowed for the creation of an algorithmic rule essentially stating that if these traits are available, these traits should be used to match across organizations.

Combination of Traits	**Completeness**	**Uniqueness**
first name, last name, date of birth, sex, and either zip code	91.1%	99.2%
first name, last name, date of birth, sex, and phone number	76.2%	99.5%

Requirements for EHRs

As above, the AMA supports a minimum set of elements that should be collected and exchanged: first name, last name, date of birth, sex, and either zip code (first 5) or phone number.

Pediatric Record Matching

Significant challenges exist with respect to neo-natal and pre-natal patient matching, including a potential lack of a name or even a birth date. Multiple birth persons present challenges with the same date of birth, address, mother's maiden name, and potentially similar names and identifiers between newborns. Moreover, newborns do not have a social security number or government-assigned identification at the time of birth. CMS should consider standard adoption; information governance, process, and technology; vendor capture of multiple birth indicator; and **creation of a medical record** prior to a birth event to handle the unique matching issues related to pediatrics.

Patient Engagement

We believe that involving the patient in data entry, correction, and maintenance can maintain and enhance patient data integrity over time. This approach includes making it a practice to ask the patient at every visit (and training staff on the value of doing so) whether their address or phone number has changed and also having the patient review their demographic information to ensure its correctness. Patient portals and other self-service applications can also help patients understand the extent of their identity completeness and how it can be increased. Accurate patient matching is a pre-requisite for the ability to enable patients to become more engaged in their data exchange.

Use of USCDI

The AMA believes that ONC should coordinate with CMS to advance more standardized data elements for patient matching by leveraging the USCDI. Additionally, ONC and CMS should work together to establish guidance surrounding common issues that could be resolved by standardization, such as the following:

- Recording names with spaces, hyphens, or apostrophes;
- Listing addresses in single or separate fields (e.g., separately street names from the city and state);
- Including special characters in phone numbers; and
- Handling missing data for fields (e.g., SSN, email address).

[38] The Sequoia Project, *A Framework for Cross-Organizational Patient Identity Management* (2018).

AMA
AMERICAN MEDICAL ASSOCIATION

JAMES L. MADARA, MD
EXECUTIVE VICE PRESIDENT, CEO

ama-assn.org
t (312) 464-5000

September 21, 2018

Scott Gottlieb, MD
Commissioner
U.S. Food and Drug Administration
10903 New Hampshire Avenue
Silver Spring, MD 20993

Re: Software Precertification Program: Working Model–Version 0.2 –June 2018

Dear Commissioner Gottlieb:

On behalf of the physician and medical student members of the American Medical Association (AMA), I appreciate the opportunity to provide comments on the most recent version of the proposed Precertification Program for software as a medical device (SaMD) and to respond to questions posed by the U.S. Food and Drug Administration (FDA). As outlined in previous correspondence, the AMA understands the compelling need to develop alternative oversight model(s) for SaMD that provide a strong incentive for developers to cultivate and maintain a culture and practice of excellence in order to ensure the design, development, validation, deployment, and modification of a safe and efficacious SaMD. This is an important effort in light of the large and rapidly growing volume of SaMD and the finite FDA resources available to provide oversight. The AMA has a number of recommendations in response to the specific questions posed by the FDA concerning the Precertification Program, as well as additional comments related to a subset of software and computer science methods and systems variously referred to as continuous machine learning, deep learning, or continuous learning systems.

The AMA urges the FDA to be very cautious with regard to the speed with which the Precertification Program is being developed. While we appreciate the efforts to engage physician organizations over the last several months, industry has been steeped in the complexities of this proposal for an extended period of time. The AMA, physician organizations, and the broader health care provider community would benefit from obtaining additional information on the experiences of the companies participating in the Precertification Program pilot as there are no public examples of how this program operates in practice to provide context since the January 2018 Workshop meeting.

SaMD Precertification Program[1]

The FDA has sought the AMA's feedback on a number of questions. The responses to the questions are contained below in the format presented by the FDA.

[1] The following comments apply to all SaMD except for "continuous learning" systems.

Q	Work stream	Question / Input	Desired Output
1.1	Excellence Appraisal	What attributes should organizations who have not developed medical devices have so they can adequately demonstrate a track record of excellence in the principles of patient safety and clinical responsibility, in particular clinical effectiveness?	As outlined in the AMA's prior comment letter, we do not support the establishment of two levels of precertification—one for organizations that have developed software and one for organizations that have not. In short, the risks and challenges associated with deploying SaMD into the health care ecosystem is challenging and rife with unanticipated and unexpected challenges. Organizations that have not successfully deployed SaMD should first demonstrate that they are able to deploy such software safely through the existing oversight product specific process. The Precertification Program will only engender the trust of SaMD end-users if it is understood that Precertification organizations have not only met and demonstrated adherence to the excellence principles, but also have a track record of having done so with SaMD. It might be appropriate at a future date to test a second level of precertification for organizations that do not have a track record, but there is a much higher risk that such organizations may market SaMD that could cause harm. This would degrade trust in the Precertification Program and fails to provide the requisite documented track record of performance that should be part of the Precertification Program.
1.2	Excellence Appraisal	Should the FDA consider weighing Patient Safety and Clinical Responsibility more heavily than the other Excellence Principles?	The AMA strongly supports weighting Patient Safety and Clinical Responsibility more heavily than the other Excellence Principles. Again, this is essential to engender trust among end-users that the Precertification Program is designed to incentivize best practices and quality that consistently and reliably drive SaMD performance anchored in patient safety and clinical factors (validity, analytical validity, reliability, etc.).
1.3	Excellence Appraisal	What "clinical standards" can be leveraged as part of the Excellence Appraisal?	The AMA supports the use of standards as long as the process is open and transparent and the AMA supports standard development organization standards, such as ISO and HL7.
4.1	Real World Performance	Should the three proposed data domains for real world health analytics be tailored to the type or risk level of SaMD product? (The three proposed data domains include:	The AMA agrees with the FDA that organizations can show excellence per the Pre-Cert Excellence Principles by taking user-centric steps toward continuous improvement through proactive monitoring of Real World Performance (RWP) data related to their SaMD products. In general, it would be reasonable to tailor the real-world health analytics to the type and risk level of the SaMD product. However, the AMA encourages the

Q	Work stream	Question / Input	Desired Output
		Human Factors and Usability Engineering, Clinical Safety, Health Benefits)	FDA to consider whether this would create confusion, particularly where such information is provided to end-users related to clinical safety and health benefit. Careful consideration should be given to cognitive burden to regulators, end-users, and other stakeholders (such as researchers) created by lack of standardization.
4.2	Real World Performance Analytics (RWPA)	Where is transparency important in the RWPA process?	The AMA urges the FDA to not use the term "transparency" in this context; it creates confusion as this term is used to address a different set of concepts in the context of continuous learning systems (which concerns data and algorithmic transparency, for example). Real world performance analytics disclosure should be required (or minimally available): (1) when an organization seeks Precertification status; (2) when a SaMD product is introduced into the market; (3) at regular established intervals after market entry, based on risk, but generally not longer than monthly; (4) when a major modification is made; and (5) when there is an adverse event.

The FDA has also sought feedback on specific real-world performance analytics (RWPA) metrics important to physicians and patients. The FDA has identified three RWPA domains including:

- Real world health analytics: human factors and usability engineering, clinical safety, and health benefits;
- User experience analytics: user satisfaction, issue resolution, user feedback channels, and user engagement;
- Product performance analytics: cybersecurity and product performance.

As a threshold matter, to the extent that developers need flexibility on metric selection within each of the above domains based on intended use, functionality, and risk classification of the SaMD product, the AMA strongly urges the FDA to consider the cognitive burden such flexibility places on end-users where there is a lack of standardization and there is not an ability to make apples-to-apples comparisons due to significant variation in selected metrics. The AMA also urges the FDA to provide stakeholders examples of how the metrics would be shared with the end-users. Metrics under all three domains should be provided to end-users based on the specific SaMD product. While organizations should provide overall performance of all products for purposes of Precertification designation to the FDA, end-users generally should have readily available relevant performance metrics that are product specific. The AMA continues to engage physicians and national medical specialties in order to provide additional feedback with regard to specific metrics.

Continuous Learning Systems and Transparency

The AMA does not support the inclusion of continuous learning systems in the Precertification Program as currently proposed. While certain machine learning systems that are static (locked) may be appropriate for the Precertification Program, there remain a wide array of additional risks and unanswered questions with regard to the safety of continuous learning systems. The concern is heightened as there is not a widely accepted methodology taxonomy and set of definitions to characterize different augmented intelligence (AI) (commonly referred to as artificial intelligence) methods. The AMA is working with experts within our organization, along with a number of other health care stakeholder organizations, to facilitate a convergence that would be consistent with the terms and method descriptors used by the broader community of AI stakeholders. For example, the most recent SaMD products that the FDA authorized and identified as utilizing AI methods do not utilize continuous learning systems. Instead, these are static (locked) systems where the algorithm does not change once subject to FDA authorization and introduction into the market. The AMA recognizes the importance of the consistent use of terms and method identification and is concerned that continuous learning systems do not fit within the current risk level identification laid out in the Precertification Program. We urge the FDA to develop a separate proposal that captures the additional risks associated with continuous learning systems and the additional controls that may need to be standard to ensure safety and efficacy. In addition, the AMA will provide additional comments under separate cover concerning transparency in the context of continuous learning systems. The concept of transparency for these types of systems is one that concerns a broad group of stakeholders as different types of transparency may be required depending on the product. In addition, specific requirements may vary over the life cycle of the continuous learning system.

We appreciate the opportunity to continue an ongoing discussion on these important reform models and concepts. If you have questions, please contact Shannon Curtis, Assistant Director, Division of Federal Affairs, at shannon.curtis@ama-assn.org or 202-789-8510.

Sincerely,

James L. Madara, MD