233 N. Michigan Ave.,21st Fl.
Chicago, IL 60601-5800

phone » (312) 233-1100
fax » (312) 233-1090
web » www.ahima.org

American Health Information Management Association®

June 3, 2019

Dr. Donald Rucker
National Coordinator
Office of the National Coordinator for Health Information Technology
330 C Street, SW
Floor 7, Mary E. Switzer Building
Washington, DC 20201

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

Via electronic submission: www.regulations.gov

Dear Dr. Rucker:

Thank you for the opportunity to provide feedback on the 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program proposed rule.

As you know, the American Health Information Management Association (AHIMA) is the national non-profit association of health information management (HIM) professionals. Serving 52 affiliated component state associations including the District of Columbia and Puerto Rico, AHIMA represents over 103,000 health information management professionals with the mission of empowering people to impact health. AHIMA's credentialed and certified HIM members can be found in more than 40 different employer settings in 120 different job functions—consistently ensuring that health information is accurate, timely, complete, and available to patients and clinicians.

We would like to offer below some general comments about the proposed rule followed by more specific comments using the public comment template provided by ONC.

## General Comments

**Scope and Definition of Electronic Health Information (EHI)**

AHIMA recognizes the compelling public policy rationale for the information blocking provision to encompass a broad range of activities. However, we are concerned about the lack of clarity and predictability around the definition of "electronic health information" as currently proposed as well as the feasibility of operationalizing such a definition. For example, would electronic health information include education records covered by the Family Educational Rights and Privacy (FERPA) Act and/or employment records? AHIMA is also concerned that because both the 21st Century Cures Act and this proposed rule do not appear to obviate the requirements under HIPAA, EHI as currently defined adds an additional layer of complexity in complying with existing definitions in current law, including individually identifiable health information (IIHI),

protected health information (PHI), and electronic protected health information (ePHI) as well as state laws that define medical information. **Therefore, at a minimum, we recommend that ONC constrain the definition of "electronic health information" to the US Core Data for Interoperability (USCDI).** We believe that constraining the definition of EHI to the USCDI establishes clear guardrails for actors as to what electronic health information must be provided for access, exchange and use. Over time, we envision that as the ONC expands the USCDI to include additional data classes and/or data elements, the definition of EHI will expand with it while continuing to provide actors with a degree of certainty as to what information must be provided in accordance with the information blocking provision. We also recommend that ONC work with the HHS Office for Civil Rights (OCR) to develop a crosswalk for the definition of EHI to protected health information (PHI) as currently defined by the Health Insurance Portability and Accountability Act (HIPAA.) Such guidance will assist HIM professionals in ensuring that they are meeting the obligations set forth under this proposed rule and HIPAA.

**Privacy and Security of Third-Party Applications**

AHIMA recognizes that the Office for Civil Rights has stated that if a patient's app was not provided by or on behalf of a covered entity, the covered entity will not be liable under HIPAA for any subsequent use or disclosure of ePHI received by the app.[1] However, we are concerned that as currently proposed, the rule does not include sufficient guardrails around HIPAA non-covered entities to protect the privacy and security of a patient's health information. Patients may be unaware that once they authorize a covered entity to push their electronic health information to a third-party app and such an entity is a HIPAA non-covered entity, the rights afforded under HIPAA no longer apply. Additionally, patients may be unaware of how an app intends to use their health information, leaving them to the mercy of the app developer's terms of service and/or privacy policy unless an act on the part of an app developer meets the "unfair or deceptive acts or practices" standard under the Federal Trade Commission (FTC) Act. In fact, a recent cross-sectional study of 36 top-ranked apps for depression and smoking cessation revealed that only 16 apps described secondary uses.[2] 81 percent of the 36 apps transmitted data for advertising and marketing purposes to two commercial entities, Google and Facebook, but only 43 percent transmitting data to Google and 50 percent transmitting data to Facebook disclosed this.[3] Failure to provide appropriate and transparent privacy and security safeguards and/or lack of flexibility in allowing actors to perform due diligence could invite opportunities for "bad actors" to enter the market and potentially use such sensitive data for nefarious activities. **Along these lines, we recommend that as part of the certification criterion, ONC should require API Technology Suppliers to verify an app's "yes/no" attestation to: (1) industry-recognized guidance such as Xcertia's™ mHealth App Guidelines, (2) transparency statements and best practices including the Federal Trade Commission's Mobile App Developers: FTC Best Practices and/or the CARIN Alliance's Code of Conduct and (3) the adoption of either ONC's Model Privacy Notice or a notice in plain language with substantially the same content as described in ONC's Model Privacy Notice.** Upon issuing a "yes" attestation, a health IT developer could in turn whitelist the app for use by an API Data Provider. We believe such a "light touch" attestation would not interfere with a provider's use of their acquired API technology and enhance a health IT developer's responsibility to patients. We also believe that such a requirement is consistent with enabling patients' access to their EHI via an API-enabled app "without special effort" as this would not impose substantial additional costs or access requirements that may impede the patient's ability to access their

[1] Available at: https://www.hhs.gov/hipaa/for-professionals/faq/572/does-a-hipaa-covered-entity-bear-liability.html.
[2] 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.
[3] Id.

information in a persistent manner. A requirement that an app attest to the adoption of a model privacy notice would also be consistent with ONC's proposed Minimum Required Terms and Conditions (MRTCs) in Draft 2 of the Trusted Exchange Framework and Common Agreement (TEFCA).[4]

**Effective Date of Information Blocking Provision**

The information blocking provision represents a fundamental shift that will require stakeholders to evolve from a mindset in which the sharing of health information is permitted under HIPAA to one in which EHI must be shared unless an exception applies under Part 171 Subpart B. Such transformation will require an appropriate transition period to ensure that stakeholders have sufficient time to revise existing organizational and business practices and policies as well as offer additional training for staff to ensure that such policies and practices do not run afoul with the information blocking provision set forth under this proposed rule. We are concerned that if ONC intends to assign the effective date of Part 171—Information Blocking as 24 months from the final rule's effective date, this will not provide sufficient time for actors to adjust to the new certification criterion and be in compliance with the information blocking provision. **For that reason, AHIMA recommends an 18 to 24-month delay of the effective date of the information blocking provision in this proposed rule.** We believe that such a delay will provide actors with the flexibility needed to make corresponding adjustments to existing business and organizational policies and practices to ensure compliance with Part 171 of this proposed rule.

**Supplemental Notice of Proposed Rulemaking**

**AHIMA also recommends that ONC consider issuing a Supplemental Notice of Proposed Rulemaking (SNPRM) to seek further comments on the information blocking provision of the 21st Century Cures Act: Interoperability, Information Blocking and the ONC Health IT Certification Program 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 EHI for authorized and permitted purposes which in turn have frustrated care coordination and improvements in healthcare 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 expansive definitions such as "electronic health information," that require additional clarification from ONC before the entire rule is finalized given the significant economic impact of this rule. Furthermore, as you know, 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[5], potential modernization of HIPAA to support and remove barriers to coordinated care, as well as enactment of the Trusted Exchange Framework and Common Agreement, all of which have immediate implications for Part 171 of this proposed rule. Issuance of an SNPRM would enable ONC to propose additional clarifications to the information blocking rule and seek feedback on its modified proposals to further address 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.

Detailed comments about specific aspects of the proposed rule can be found in **Appendix A.** We appreciate the opportunity to submit comments on the 21st Century Cures Act: Interoperability, Information Blocking, and the Health IT Certification Program proposed rule. We hope that you will continue to engage extensively

[4] Available at: https://www.healthit.gov/sites/default/files/page/2019-04/FINALTEFCAQTF41719508version.pdf.
[5] Available at: https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=201810&RIN=0930-AA32.

with stakeholders on the proposed rule and we look forward to working with you to ensure its successful finalization and implementation. Should you or your staff have any additional questions or comments, please contact Lauren Riplinger, Senior Director, Federal Relations, at lauren.riplinger@ahima.org and (202) 839-1218.

Sincerely,

Dr. Wylecia Wiggs Harris, PhD, CAE
Chief Executive Officer
AHIMA

# *Appendix A: ONC Proposed Rule Public Comment Template*

## *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:**

In general, AHIMA supports the adoption of USCDI, Version 1 (v1) at §170.213. We agree with ONC that the USCDI will increase the minimum baseline of data classes that health IT developers must make available for interoperable exchange, and we believe the USCDI contains important elements in helping to treat patients more effectively. That said, we are concerned that the USCDI v1 does not correlate to content exchange standards and implementation specifications. Lack of constrained interpretation of standards under the CCDS has led to long-standing concerns among data professionals including variation in data governance policies among electronic health record (EHR) systems as well as subsequent difficulties in exchanging electronic health information. We are concerned that allowing the USCDI v1 to be "context exchange" standard agnostic will compound these difficulties as future data classes and/or elements are added.

With respect to the inclusion of new data classes and/or elements to be included in the USCDI v1, we support the inclusion of demographic data elements such as "address" and "phone number" as we believe that these are necessary data elements for interoperable exchange and patient matching. A 2015 study conducted by Intermountain Healthcare found that the collection of certain data elements including ZIP codes in coordination with the collection of regularly captured demographics such as last names resulted in higher patient matching rates.[6] However, additional opportunities exist to capture such demographic data elements accurately at the source. Along these lines, we recommend, at a minimum, that ONC support the standardization of demographic data elements where well-tested

[6] Available at: https://www.pewtrusts.org/en/research-and-analysis/reports/2018/10/02/enhanced-patient-matching-critical-to-achieving-full-promise-of-digital-health-records.

semantic standards exist and could be widely implemented in EHR technology. More specifically, we recommend that ONC specify the US Postal Service standard for "address" under the USCDI. A recent study indicates that use of the US Postal Service standard could improve match rates by 2-3 percent.[7] Evidence suggests that further standardization of "last name" and "address" could improve the match rate further by as much as 8 percent.[8]

AHIMA also recommends that ONC work with industry and experts to identify other regularly collected demographic data elements that could be incorporated into the USCDI. For example, the availability of an email address in a patient's record has increased over time from 8.94 percent in 2005 to 54.08 percent in 2014.[9] Email addresses could serve as another critical datapoint in accurately matching a patient to their health information.

AHIMA also recommends that self-reported gender identity be included as a required patient demographic data element in the USCDI. Accurate identification and awareness of a patient's gender status is vital to accurately identifying a patient and ensuring continuity of care.[10] Furthermore, lack of awareness of a patient's gender identity raises significant patient safety concerns. If a clinician is unaware of a patient's gender identity, he or she may miss an opportunity to offer specific screenings to support the patient either physically or emotionally as gender often drives template tools designed specifically for male or female patients and may drive alerts and/or suggestions for diagnostic testing in EHRs.[11] Such an inclusion also aligns with 2015 Edition demographics certification criterion at §170.315(a)(5).

We believe that additional opportunities exist beyond the USCDI to improve patient matching rates and accurate patient identification. Additional recommendations can be found in **Section X—Patient Matching Request for Information.**

AHIMA also supports the inclusion of new data classes such as clinical notes in the USCDI v1. Clinical notes are critical for improved care coordination yet are often missing during electronic health information exchange. We are pleased that the USCDI v1 includes eight note types for both inpatient and outpatient settings, and we hope that the USCDI may be expanded in the future to include other clinical notes that meet the clinical and communication needs of clinicians and service providers that are not hospital based or in ambulatory care practices such as long-term, post-acute care settings.

AHIMA also supports the inclusion of "provenance" as a new data class in the USCDI v1. We agree with ONC that this metadata is critical to improving the trustworthiness and reliability of the data being exchanged. That said, we support the USCDI Task Force's recommendations that "agent/entity" be used instead of "author/author organization." We believe such a change would be more consistent with existing standards. We also recommend that ONC consider adding additional provenance elements such as the identity of the individual or entity that the data was obtained from or sent by once industry consensus is achieved in defining provenance in a standardized manner. From a health information professional perspective, we believe the addition of such elements would greatly enhance

[7] Grannis, Shaun J. et al., "Evaluating the effect of data standardization and validation on patient matching accuracy," *Journal of the American Medical Informatics Association* 26, no. 5 (May 2019): 447-456, https://doi.org/10.1093/jamia/ocy191.
[8] Id.
[9] Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6241737/.
[10] Deming, Sally; Dooling, Julie A; Kadlec, Lesley; Kirby, Annessa; Munns, Megan. "Treating LGBT Status as a Patient Safety Issue" *Journal of AHIMA* 87, no.4 (April 2016): 36-37. http://bok.ahima.org/doc?oid=301414#.XL4XAlVKhEa.
[11] Id.

the trustworthiness and reliability of the data being exchanged, particularly in instances where the "agent/entity" may not be a clinician such as scribes.

**§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:**

AHIMA recognizes that having the functionality to efficiently export entire electronic health records (EHRs) for all patients in a computable, electronic format will help facilitate providers' ability to switch health IT systems and migrate electronic health information (EHI) for use in other technologies. Additionally, we support efforts to enable the export of a single patient's electronic health information upon a valid request from the patient or a user on the patient's behalf. AHIMA continues to champion efforts that clarify an individual's right to access their health information and enhance the ability to obtain such access while improving workflow for HIM professionals who are often tasked with fulfilling such requests.

That said, we would like to offer a number of recommendations around the EHI export criterion.

First, we believe that the rule's current proposal to require EHI export to apply to a health IT's "entire database" lack clarity. For example, it is unclear from the preamble whether data acquired from third parties including patient-generated health data that might be stored separately in data lakes should fall within the scope of a health IT system's entire database. We recommend that ONC provide clarity in the final rule preamble around the scope of the EHI export in the 2015 Edition certification criteria. Additionally, we agree with the HITAC's Conditions and Maintenance of Certification Task Force that health IT developers be required to provide a plain language definition of EHI typically included in the legal medical record held by their certified health IT module as part of their export documentation. Furthermore, we also recommend that health IT developers attest or publish as part of the export format documentation the types of EHI they cannot support for export. We believe that such a requirement will help clinicians in selecting a health IT system that has the functionality to meet the specific uses cases that § 170.315(b)(10) seeks to address.

We are also concerned about ONC's definition of "timely" in §170.315(b)(10)(A). We understand from the preamble that "timely" does not mean real time and that any delays in providing the export must be "no longer than reasonably necessary to avoid interference with other clinical functions of the health IT system." However, we recommend that ONC make clear in the preamble that in the patient access context, health IT developers should not delay in providing the export to the user beyond the outer limits allowed under HIPAA for an individual right of access request. Such clarification will help ensure that if a user relies on the EHI export functionality to fulfill a patient access request under HIPAA, the user will not be in non-compliance with HIPAA due to delays on the part of the health IT developer.

Finally, AHIMA believes that with respect to both use cases under §170.315(b)(10), requiring health IT systems to adopt criterion that includes capabilities that allow providers to set arbitrary timeframes for EHI export would be contrary to the individual right of access under HIPAA and the intent of section 4006 of the 21st Century Cures Act that patients have "access to their electronic health information in a single longitudinal format."[12][13] We are also concerned that such functionality could implicate the information blocking provision and be deemed as a practice that interferes with the access, exchange and use of EHI by limiting the utility or value of the EHI by diminishing the completeness and/or quality of the data.

[12] P.L. 114-255.

[13] Available at: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html.

## *Section VIII – Information Blocking*

## 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:**

AHIMA supports the inclusion of the preventing harm exception under §171.201. Such an exception is critical in helping to ensure the quality and integrity of the data being accessed, exchanged and used. HIM professionals often encounter instances where due to a failure of health IT technology, integration of electronic health information may lead to a risk of corrupt or inaccurate data being incorporated into a patient's EHR and/or misidentification of a patient or a patient's EHI. A recent example involved the consolidation of two hospitals in which a 10-character limitation in the "First Name" and "Last Name" fields within an electronic health record (EHR) at one of the facilities led to an inability to utilize patient matching algorithms because the other institution had a 14-character limitation in its "First Name" and

"Last Name" fields within its separate EHR. Had the HIM department not identified the technology limitation and instituted a manual review of 11,000 names that were greater than 10 characters, such integration could have led to inaccuracies in the patient's record and in turn may have jeopardized patient safety.

## § 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 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
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:**

AHIMA supports the inclusion of an exception at §171.202 to promote the privacy of EHI. In particular, we support ONC's inclusion of the sub exception at §171.202(d) and its alignment with the requirements under HIPAA as well as ONC's recognition of an individual's express privacy preferences under §171.202(e). However, we recommend that ONC provide guidance regarding what could be considered a "reasonable time period" under §171.202(e)(3) to provide additional clarity to health information professionals that will be tasked with documenting the individual's privacy preferences in accordance with the rule.

Additionally, AHIMA offers the following recommendations to improve §171.202 as currently proposed.

First, we recommend that the preamble make clear that privacy practices required by law and that subsequently do not implicate the information blocking provision include state laws. While the preamble offers examples of circumstances under HIPAA where an actor is required by law not to exchange an individual's PHI, we believe that it would be helpful to provide additional examples where state law may explicitly prohibit the sharing of health information but will not implicate the information blocking provision.

Second, it is unclear from the proposed rule where, under §171.202(b) in instances where federal and/or state laws require a precondition to be satisfied and the precondition has not been met whether the actor is obligated to provide access, exchange and use of EHI unrelated to the precondition to avoid implicating the information blocking provision. For example, a patient's EHI contains substance use disorder health information covered by 42 CFR Part 2 and an actor does not have a patient's consent to disclose or re-disclose the patient-identifying information related to the individual's substance use disorder. Is the actor still obligated to provide access, exchange, and use of EHI unrelated to the individual's substance use disorder to avoid implicating the information blocking provision, or will the actor not be required to provide access, exchange and use to *all* of a patient's EHI, provided it meets the requirements under the sub exception? The 42 CFR Part 2 regulation continues to present operational challenges for HIM professionals working in designated Part 2 programs. While many HIM professionals working in such programs are often forced to work with paper records, in instances where a Part 2 program may have an EHR, data segmentation functionality is often not available. We are concerned that requiring actors to still send EHI not covered by a precondition to avoid implicating the information blocking provision would create an immense burden for health information professionals tasked with having to separate out Part 2 or other sensitive health information from other EHI. We therefore ask ONC to clarify that an actor would not be obligated to share all EHI if an actor meets the sub exception requirements under §171.202(b).

Third, the preamble lacks sufficient clarify as to how the minimum necessary standard under HIPAA intersects with this exception. In particular, it is unclear the extent to which the sub exceptions under §171.202 account for the obligation for covered entities and/or business associates to meet the minimum necessary standard under HIPAA. For instance, under sub exception §171.202(b), the examples provided in the preamble demonstrate how not satisfying a precondition, subject to certain conditions will not be considered information blocking under the proposed rule. We understand that the preamble states clearly that under sub exception §171.202(b) "where the satisfaction of a precondition relies solely on an actor, such as the minimum necessary determination made under HIPAA . . . the actor's policies and procedures would need to particularize the steps that the actor will take in order to ensure that it satisfies the precondition."[14] However, it is unclear from the preamble if an actor was seeking to meet the minimum necessary standard, what the precondition is that has not been satisfied as to allow the actor to take advantage of the exception. We recommend that ONC create an additional sub-exception under §171.202 for actors that are covered entities and business associates who are required to meet the minimum necessary standard under HIPAA. Under such a sub-exception, the actor would not implicate the information blocking provision in complying with minimum necessary only when the EHI is ePHI and provided the actor's practice meets the conditions under §171.202(b)(1) and (b)(3).

**§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

[14] Available at: https://www.govinfo.gov/content/pkg/FR-2019-03-04/pdf/2019-02224.pdf.

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

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:**

AHIMA supports ONC's intent under this exception to not dictate a specific security approach given the rapidly changing security landscape. Along these lines, we recommend that ONC clarify that an actor may use and adopt security policies and/or practices that exceed those required by law based on their assessment of the threat environment and provided the practice meets the conditions required under §171.203.

**§ 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

(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:**

In general, AHIMA is concerned about the ambiguous nature of the infeasibility exception. We agree with

ONC that there are legitimate circumstances beyond an actor's control that may limit its ability to comply with requests for access, exchange and use and therefore an actor should be able to decline such a request without implicating the information blocking provision. However, we are concerned that the exception contains a number of undefined terms including "burden," "timely," and "reasonable alternative" which could create uncertainty for actors in whether they meet the requirements under the exception until after the fact. In turn, such uncertainty could dissuade actors from taking advantage of this critical exception.

Additionally, AHIMA is concerned that this exception does not fully consider potential conflicts between valid contracts such as Business Associate Agreements and subsequent requests for data access, exchange, and use that are inconsistent with these contracts. We recognize that in determining the "unreasonableness" for an actor in assuming the burden of providing access, exchange and use, ONC proposes to rely on several key factors including whether the actor maintains ePHI on behalf of a covered entity at §171.205(a)(1)(vi). However, it is unclear from the proposed rule and the preamble the extent to which existing contractual obligations meet the infeasibility exception.

## *Section X – Patient Matching Request for Information*

| **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:** Not applicable |
| **Public Comment Field:**<br><br>AHIMA supports ONC's intent to identify additional opportunities in the patient matching space and explore ways that ONC can lead and contribute to coordination efforts with respect to patient matching. Today, there is no consistent approach to accurately matching a patient to their health information which has led to significant costs to hospitals, health systems, physician practices, long-term, post-acute care (LTPAC) facilities, and other providers. According to a 2016 study of healthcare executives, misidentification costs the average healthcare facility $17.4 million per year in denied claims and lost revenue.[15] Lack of a consistent and accurate approach to patient matching has also hindered the advancement of health information exchange across the care continuum. A 2017 study by the American Hospital Association indicates that 45 percent of large hospitals reported that difficulties in accurately identifying patients across health information technology (health IT) systems limits health information exchange.[16] More importantly, there are patient safety implications when data is matched to the wrong patient and when essential data is lacking from a patient's record due to identity issues. Patient matching errors can often begin at registration and can generate a cascade of errors including wrong-site surgery, delayed or lost diagnoses, duplicative testing, and wrong patient orders. According to the *2016 National Patient Misidentification Report,* 86 percent of respondents said they have witnessed or know of a medical error that was the result of patient misidentification.[17]<br><br>We offer the following comments in response to the questions posed by ONC in this Request for Information (RFI).<br><br>**<u>Effect of Data Collection Standards on the Quality of Health Data and Patient Matching</u>** |

[15] 2019 National Patient Misidentification Report, Available at: https://pages.imprivata.com/rs/imprivata/images/Ponemon-Report_121416.pdf.
[16] AHA, Trendwatch: Sharing Health Information, Available at: https://www.aha.org/system/files/2018-03/sharing-health-information.pdf.
[17] 2019 National Patient Misidentification Report, Available at: https://pages.imprivata.com/rs/imprivata/images/Ponemon-Report_121416.pdf.

We agree with ONC that even the most advanced technologies cannot eliminate the risk of human error that often leads to data quality issues. In general, AHIMA supports data governance and data quality improvement policies and procedures that are fundamental to improving overall patient matching rates and data integrity. As mentioned in our comments in Section IV concerning the USCDI, we recommend that ONC support the adoption of well-tested demographic data standards to improve patient matching including requiring the use of the US Postal Service standard for "address" under the USCDI. Additionally, there are a number of standardized primary and secondary data attributes that could help facilitate accurate patient matching including NCVHS' "Core Health Data Elements," Accredited Standards Committee X12 (ASCX12)'s Basic Character Set, and CAQH standards. We refer ONC to an AHIMA publication which outlines these attributes in greater detail.[18] AHIMA also recommends that ONC work with industry to identify other well-tested data collection standards that could be adopted under the USCDI.

**Solutions that May Increase the Likelihood of Accurate Data Capture**

Data governance and data quality improvement policies are essential to improving overall patient matching rates and core to data integrity in general. As part of the Medicare and Medicaid Program; Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans in Federally-facilitated Exchanges and Health Care Providers proposed rule, we have recommended that CMS require, at a minimum, Medicare FFS, MA Plans, Medicaid FFS, Medicaid managed care plans, CHIP FFS, CHIP managed care entities and QHP issuers in FFEs to annually evaluate their patient demographic data management practices using the Office of the National Coordinator (ONC)'s Patient Demographic and Data Quality (PDDQ) Framework. Plans could also be required to submit to CMS its scores in the five PDDQ process areas—data governance, data quality, data operations, platform and standards, and supporting processes—to demonstrate its overall data management practices. As ONC proposes under TEFCA Draft 2 to require Qualified Health Information Networks (QHINs) to annually evaluate their patient demographic data management practices using the PDDQ Framework, ONC, operating through the Recognized Coordinating Entity (RCE), could also require QHINs to submit (in a non-punitive manner) their scores in the five PDDQ process areas to evaluate data management practices. Such a requirement could help establish a benchmark by which to measure the extent of the problem and whether data quality improvements have been made on a year-to-year basis. Alternatively, ONC could make public these scores much like CMS' Physician Compare for which Participants, Participant Members and/or Individual Users may use to evaluate its participation in a QHIN.

**Requirements for EHRs to Assure Accurateness and Completeness of Data Collected for Patient Matching**

As noted in our comments under the Preventing Harm exception at §171.201, lack of standardization in data fields can often lead to potential patient matching errors and require manual review of records to prevent such instances from occurring. Standardized data fields that do not limit the number of characters or that do not allow users to bypass certain required demographic data elements (including those elements collected at the time of registration) could increase the likelihood of accurate data capture.

[18] Katherine G. Lusk, MHSM, RHIA; Neysa Noreen, RHIA; Godwin Okafor, RHIA, FAC-P/PM, FAC-COR; Kimberly Peterson, MHIM, RHIA, CHTS-TS; and Erik Pupo, MBA, CPHIMS, FHIMSS, "Patient Matching In Health Information Exchanges," *Perspectives in Health Information Management,* Available at: https://perspectives.ahima.org/patient-matching-in-health-information-exchanges/.

**Innovative and Effective Technical or Non-Technical Approaches that Support Accurate Pediatric Patient Record Matching**

We agree with ONC that there are unique patient matching issues specific to pediatrics such as newborns that have not yet received their legal name and have a temporary name, patients that are a product of a multiple birth delivery that are named similarly, and newborns that lack a Social Security Number (SSN) or government identification at the time of birth. We believe there are a number of policies and practices currently in use by healthcare organizations that could be leveraged to support pediatric patient record matching including a standardized naming convention for temporary newborn names. The standardized naming convention for temporary newborn names would look like the following—

- Mom's name: ***Katie Smith***
- Mom's maiden name: ***Katie Miller***
- Baby's name if she had a girl: ***Smith, Girl Katie***
- Baby's name if she had a boy: ***Smith, Boy Katie***
- Baby's name if she had an undetermined sex: ***Smith, Baby Katie***
- If the mom has twins: ***Smith, Girl A Katie, Smith Boy B Katie***

Such a practice would be consistent with the Joint Commission's National Patient Safety Goal (NPSG) 01.01.01 which became effective January 1, 2019.

Important considerations in using a standardized naming convention include instances where a baby may be adopted, or the baby is deemed a safe haven baby. Under the former, a birth mother's last name would be used in the temporary naming convention until the adoption is finalized and a legal name is given. Changing the temporary name to a legal name should be completed prior to discharge to avoid confusion with downstream system processing while the patient is still in the hospital. With respect to the latter, a special naming convention should be considered where the patient could be identified by—

- ***BABY***, followed by the facility abbreviation for the last name,
- ***SH*** (for "safe haven") followed by
- ***DATE*** (mm/dd/yy format) and
- ***TIME*** for the first name

For example, a patient treated at facility XYZ 11:15 am on April 30, 2019 would be name: BABYXYZ, SH0430191115.

Other practices and policies that could be further disseminated include capturing and using a mother's maiden name, maintaining the temporary newborn name as an "alias," multiple birth designation and multiple birth order in patient matching and linking of records to increase the data available for algorithms or visual matching to enhance patient matching.

**Patient Matching Solutions Involving Patients**

We agree with ONC that involving patients in patient matching could be a viable and effective solution to increase the accuracy of matching while giving patients access to their own clinical information. We recommend that as ONC explores different methods and technical platforms that seek to include

patients that it take into consideration key barriers that may inhibit certain patient populations from being able to participate in the capture, updating and maintenance of their own demographic and health data including race and ethnicity, age and socioeconomic status.

**Standardized Metrics for Evaluation of Algorithm Performance**

AHIMA supports the voluntary adoption of a set of agreed upon metrics to evaluate algorithm performance across the industry. Such benchmarking will help shed further light on the extent of the variation in matching algorithms and offer health IT developers an opportunity to improve upon their algorithms. We believe any set of agreed upon metrics should be developed by the industry in partnership with ONC. ONC should consider whether once developed the metrics could be integrated into the certification criterion under its Health IT Certification Program whereby a health IT developer could attest its assent to the agreed upon standardized metrics.

**Transparent Patient Matching Indicators Including Database Duplicate Rate, Duplicate Creation Rate and True Match Rate**

AHIMA agrees with ONC that there is a current lack of consensus, adoption and transparency of such indicators as the database duplicate rate, the duplicate creation rate and the true match rate. A survey conducted by AHIMA in 2016 revealed that 45 percent of respondents noted that they did not know their duplicate medical record rate at their facility.[19] However, given that matching rates are currently calculated differently across institutions, comparing these different rates could present challenges. Similar to above, we recommend that a set of metrics be developed by industry stakeholders in partnership with ONC to evaluate database duplicate rate, duplicate creation rate and true match rate. Furthermore, if ONC were to require these rates to be reported, we would recommend that these rates be reported voluntarily to a Patient Safety Organization (PSO) on a privileged and confidential basis. Submission of such indicators to a PSO would allow an institution and clinicians to provide such information in a blame-free environment while allowing the PSO to detect nationwide trends and insights into such data.

**Data that Could be Added or Constrained in the US Core Data for Interoperability (USCDI) to Support Patient Matching**

As noted in Section IV, AHIMA recommends that ONC work with industry and experts to identify other regularly collected demographic data elements that could be incorporated into the USCDI. For example, the availability of an email address in a patient's record has increased over time from 8.94 percent in 2005 to 54.08 percent in 2014.[20] Email addresses could serve as another critical datapoint in accurately matching a patient to their health information.

AHIMA also recommends that self-reported gender identity be included as a required patient demographic data element in the USCDI. Accurate identification and awareness of a patient's gender status is vital to accurately identifying a patient and ensuring continuity of care.[21] Furthermore, lack of awareness of a patient's gender identity raises significant patient safety concerns. If a clinician is unaware of a patient's gender identity, he or she may miss an opportunity to offer specific screenings to support the patient either physically or emotionally as gender often

[19] Dooling, Julie A; Fernandes, Lorraine M.; Kirby, Annessa; Kadlec, Lesley; Landsbach, Grant; Lusk, Katherine; Munns, Megan; Noreen, Neysa; O'Connor, Michele. "Losing the Match Game: Study Reveals Gaps in HIM's Patient Identity Integrity Practices" *Journal of AHIMA* 87, no.10 (October 2016): 39-47.
[20] Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6241737/.
[21] Deming, Sally; Dooling, Julie A; Kadlec, Lesley; Kirby, Annessa; Munns, Megan. "Treating LGBT Status as a Patient Safety Issue" *Journal of AHIMA* 87, no.4 (April 2016): 36-37. http://bok.ahima.org/doc?oid=301414#.XL4XAlVKhEa.

drives template tools designed specifically for male or female patients and may drive alerts and/or suggestions for diagnostic testing in EHRs.[22] Furthermore, such an inclusion aligns with 2015 Edition demographics certification criterion at §170.315(a)(5).

[22] Id.