May 15, 2019

Seema Verma
Administrator
Centers for Medicare & Medicaid Services
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Don Rucker, M.D.
National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

Dear Administrator Verma and Dr. Rucker:

The College of Healthcare Information Management Executives (CHIME) together with our affiliate organizations, the Association for Executives in Healthcare Information Technology (AEHIT) and the Association for Executives in Healthcare Information Applications (AEHIA), are pleased to offer our comments on the Centers for Medicare & Medicaid Services' (CMS) rule, "**Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans in the Federally-facilitated Exchanges and Health Care Providers**," and the Office of the National Coordinator for Health IT's (ONC) rule, "**21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program**." Given the intertwined nature of the topics addressed in the rules, we have elected to submit a combined comment letter for consideration by the Administration.

CHIME is an executive organization comprised of chief information officers (CIOs), chief medical information officers (CMIOs), chief nursing information officers (CNIOs), chief innovation officers, and other senior health information technology leaders at clinics and hospitals across the nation. Under the CHIME umbrella, our affiliate organizations AEHIT and AEHIA were both launched in 2014. AEHIT's members are healthcare's chief technology officers and AEHIA's members are healthcare's senior IT applications leaders. Together our nearly 4,000 CHIME, AEHIT and AEHIA members are devoted to improving the healthcare delivery experience for patients through technology.

I. Speeding Interoperability Across the Healthcare System for Patients and Providers

Our members strongly support an interconnected healthcare system whereby clinicians have timely access to the medical records and necessary patient information at the point of care. We furthermore recognize the imperative for patients to have easy and timely access to their medical information and data in a manner that is easily understood to best care for themselves and their family members. **CHIME thus strongly supports the overall intent of the CMS and ONC rules and the promise these portend for pushing the industry forward.**

In order to further strengthen CMS and ONC's proposals and to better support the interoperability intent underlying these rules, will be a need to thoughtfully sequence certain components such that: 1) vendors and providers have adequate development time; 2) greater upfront emphasis is placed on building provider capacity to utilize data received; and 3) ensuring adequate outreach and education initiatives are provided to providers and patients. Outlined below are our detailed recommendations for ensuring the vision laid out by the Administration can best be accomplished.

II. Key recommendations

Following the overview of our top recommendations is a detailed discussion of each in the body of our letter.

1. **Interim Final Rules:** Given the magnitude of changes encompassed in these rules, CMS and ONC should publishing interim final rules rather than final rules to allow additional opportunity for stakeholder comments;
2. **Timelines:** We recommend CMS and ONC provide additional time that is sequenced from the date the rule is finalized to allow stakeholders/affected entities to work toward compliance:
   a. **Certified technology:** ONC should offer at least 36 months for providers and to absorb the changes associated with changes to certified technology;
   b. **ADT:** CMS should allow at least 36 months for providers to make the admission, discharge and transition (ADT) changes;
3. **Information Blocking:** We recommend ONC take into account the following:
   a. **Penalties:** Providers should not be subjected to penalties reserved for other actors;
   b. **Definition of Actors:** App developers, companies managing the app ecosystem, and prescription drug monitoring programs (PDMPs), should be required to meet information blocking requirements;
   c. Electronic Health Information (EHI): EHI should be limited to what is contained in a certified product that is part of the legal medical record;
   b. **Exception #2, sub-exception #1:** Administrative burdens on providers should be carefully weighed in relation to the totality of administrative requirements. Changes should be completely aligned with the Health Insurance Portability and Accountability Act (HIPAA) and if there are divergences, they must be clearly reconciled;
   c. **Exception #3:** Security concerns must be more thoroughly probed, such as how providers are expected to know what kind of risks they are undertaking when connecting with APIs.
4. **Patient Identification:**
   a. ONC require vendors to share their patient matching rates with providers as part of their Maintenance of Certification (MOC);
   b. CMS should make claims data available to providers through a FHIR-based API to further patient matching;
   c. ONC should support the standardization of some demographic data, particularly applying the U.S. Postal Service Standard to the address field;
   d. We support CMS expanding the use of the Medicare ID number and recommend ONC add it to the USCDI;
5. **Health IT and Support for the Care Continuum:**
   a. More emphasis on receiving providers' ability to ingest data is needed;
   b. In fostering information sharing, a "carrot" rather than a "stick" approach is needed;
6. **2015 Certification:** We recommend ONC:
   a. **Edition:** Adopt an entirely new Edition for certification rather than updating the 2015 Edition;
   b. EHI Export: Limit the scope of EHI for export to what is contained in a certified product that is part of the legal medical record;
7. **Conditions and Maintenance of Certification (MOC):** We recommend ONC:
   a. **Communications:** Largely adopt their communications proposal as we strongly support removing restrictions vendors place around communications;
   b. **FHIR:** Adopt Release 4 with a three-year timeline;

c. **APIs:** Require app management companies to obtain a business associate agreement (BAA) with providers or establish a safe harbor for providers in the event data is released by a third-party app which was not intended by the patient;
d. **Real World Testing**: Place more focus on the ability to ingest data is needed, including requiring vendors be able to accept and ingest their own CCD;

III. Information Blocking

ONC proposes to define information blocking as a practice that is likely to interfere with, prevent or materially discourage access, exchange, or use of electronic health information (EHI). Throughout the rule, by offering hypothetical practices that could implicate this practice, ONC demonstrates the scope and breadth of the information blocking provision. However, ONC also makes clear that it has not attempted to catalog a full list of all potential types of practices that may raise information blocking concerns.

We are supportive of the intention behind 21st Century Cures Act provisions that promote information sharing and prohibit practices which aim to restrict data by purposefully not sharing patient information. These actions harm the health of the general population by impeding patients' and providers' access to treatment information, including during emergent situations when timely access is imperative. Stymying access to patient information also subjects patients to duplicative tests, (i.e. lab work and imaging), creating unnecessary costs and unneeded stress for patients.

CHIME furthermore appreciates the significant thought that has already been devoted to crafting the seven information blocking exceptions. We offer the following series of recommendations, which we believe will facilitate the implementation of this important Cures provision.

A. Enforcement of Provider Actors & Disincentives

Congress outlines four sets of actors subject to the information blocking provisions contained in Section 3022 of the Cures Act: 1) providers; 2) health IT developers; 3) health information exchanges (HIEs); and 4) health information networks (HINs). Congress furthermore outlines a penalty structure; one for providers, and other for the remaining three sets of actors.

CHIME strongly supports an environment where data sharing is encouraged, however, we believe this must be accomplished for providers without also creating disincentives to their participation. Specifically, under no circumstances do we believe that providers should be subjected to penalties set aside for vendors, HIEs, or HINs, which can be as high as $1 million per violation in civil monetary penalties. It is clear that Congress set up a distinct penalty structure specifically reserved for providers. The statute clearly articulates that providers charged with information blocking "shall be referred to the appropriate agency to be subject to appropriate disincentives using authorities under applicable Federal law, as the Secretary sets forth through notice and comment rulemaking." Additionally, many providers are already subject to substantial penalties under the Promoting Interoperability program if they fail to meet the program's requirements, which can be hundreds of thousands to millions of dollars.

Even if a provider is acting – in addition to serving primarily as a provider - as one of these other three types of actors, they should not be subject to the penalties reserved for developers, HIEs and HINs. Subjecting them to the

up to $1 million per information blocking penalty creates significant risks to the healthcare system. For example, if providers acting in any of these additional capacities are subjected to these civil monetary penalties, there could be unintended consequences, especially for smaller and mid-sized providers who could deduce that if they will be treated as an HIE they may not be able to withstand a $1 million penalty. We worry a punitive policy of this nature could also further diminish rural provider access and could unintentionally lead to additional hospital consolidation. Last, we believe this proposal would conflict with the Administration's intentions to bolster competition in the HIT marketplace.

Recommendations:

1. **Providers should not be subject to the penalty structure reserved in the Cures Act for developers, HINs and HIEs. Congress explicitly established a separate penalty structure for providers. Even when a provider is acting in additional capacities such as self-developers or HIN, they are doing so to foster patient care and should not be subjected to fines clearly reserved for these other types of actors;**
2. **While we understand that the enforcement / penalty rules for providers have not yet been outlined, we strongly recommend that providers and other actors be offered an appeals process; and**
3. **Special compensation must be made for providers who were carved out of HITECH and thus ineligible for EHR incentives. They will need more time to come into compliance since many do not have certified technology.**

B. Definition of Actors Subjected to Information Blocking

i. Healthcare Providers

The Cures Act does not define the term healthcare provider. For the purposes of information blocking, ONC has proposed to adopt the definition contained in section 3000(3) of the Public Health Service Act (PHSA) which is defined to mean:

> *The term 'health care provider' include a hospital, skilled nursing facility, nursing facility, home health entity or other long term care facility, health care clinic, community mental health center (as defined in section 1913(b)(1)), renal dialysis facility, blood center, ambulatory surgical center described in section 1833(i) of the Social Security Act, emergency medical services provider, Federally qualified health center, group practice, a pharmacist, a pharmacy, a laboratory, a physician (as defined in section 1861(r) of the Social Security Act), a practitioner (as described in section 1842(b)(18)(C) of the Social Security Act), a provider operated by, or under contract with, the Indian Health Service or by an Indian tribe (as defined in the Indian Self-Determination and Education Assistance Act), tribal organization, or urban Indian organization (as defined in section 4 of the Indian Health Care Improvement Act), a rural health clinic, a covered entity under section 340B, an ambulatory surgical center described in section 1833(i) of the Social Security Act, a therapist (as defined in section 1848(k)(3)(B)(iii) of the Social Security Act), and any other category of health care facility, entity, practitioner, or clinician determined appropriate by the Secretary.*

ONC notes this definition is different from the definition of "health care provider" under the HIPAA[1] Privacy and Security Rules, which includes providers of services, a provider of medical or health services, and any other person or organization who furnishes, bills, or is paid for healthcare in the normal course of business. ONC notes they are considering adjusting the information blocking definition of "health care provider" to cover all individuals and entities covered by the HIPAA "health care provider" definition. Together, these definitions include (but are not limited to) services delivered by a: physician; hospital; outpatient physical therapy; outpatient occupational therapy; rural health clinic; federally qualified health center; home dialysis; physician assistant; nurse practitioner; clinical psychologist; clinical social worker; nurse practitioner; clinical nurse specialist; certified nurse-midwife; qualified psychologist; durable medical equipment provider; and ambulance.

Our chief concern with the definition proposed by ONC rests with the ability of those healthcare providers who did not qualify for incentives under the Health Information Technology for Economic and Clinical Health (HITECH) Act to be able to immediately absorb the costs associated with meeting information blocking provisions. As outlined under our discussion of information blocking exceptions 4 and 5 below, in many cases these providers may not have certified EHRs.

Recommendation: There must be a ramp-up period / glide path for those providers who did not qualify for HITECH's EHR incentives, especially those who do not currently have certified products.

ii. Health IT Developers

The Office of Inspector General (OIG) may investigate information blocking claims regarding a health information technology developer of *certified* health information technology or other entity *offering* certified health information technology. In the preamble to its proposed rule, ONC writes that it does not believe the Cures Act limits the regulatory authority to link the information blocking provision with *only* the performance or use of certified health IT. Therefore, the proposed rule would also allow for the information blocking provisions to be implicated by any practice of an individual or entity that develops or offers certified health IT that is likely to interfere with the access, exchange, or use of EHI, including practices associated with *any* of the developer or offeror's health IT products that have *not* been certified under the Program.

We are aware of a drafting discrepancy in the statute that impacts oversight and enforcement of the information blocking requirements. Under section 3022(a)(1)(B), Congress discusses the four sets of actors required to meet information blocking requirements. This section describes vendors as "health IT developers." However, under Section 3022(b) which addresses enforcement of such actors, Congress refers to vendors as "health IT developers of certified products." It appears that based upon this discrepancy ONC has proposed that it would not apply the information blocking rules to vendors who have no products on the Certified Health Product List (CHPL).

We respectfully disagree with ONC on this point and urge the agency to reconsider its approach for two reasons. First, given the heavy emphasis on application programming interfaces (APIs), the way by which patients and providers are expected to access more nimbly patient information, that it seems highly unlikely that Congress intended to leave off this enormous and growing segment of the vendor community. Ensuring patients have their data in a useable format is important and will modernize the healthcare industry, helping to bring it on par with so many others that already have a robust app ecosystem. It is important to recognize, however, that health data,

[1] https://www.ssa.gov/OP_Home/ssact/title18/1861.htm

whether governed by HIPAA or not, will potentially be requested by patients using app developers who are not regulated and who wish to access patient data for a variety of purposes. By carving out all vendors who do not have product(s) on the CHPL, ONC's proposal fails to capture a significant number of vendors. We are concerned that this differential treatment is inequitable, thereby creating a parallel but significantly different set of rules. In other words, as proposed, the rule would require some developers to abide by the ONC rules, yet a separate and largely ungoverned marketplace would exist for others like technology giants and those managing the app ecosystem.

Additionally, we have strong concerns that without adequate oversight of this segment of the vendor community, patients may be incredibly vulnerable. One only needs to read the daily headlines to see the barrage of complaints citizens have filed with the Federal Trade Commission (FTC) and others around inappropriate and secondary uses of their information – in some cases healthcare information. Many other citizens remain largely unaware – even if they have unwittingly agreed – that their data is being shared and reused. A strong regulatory framework needs to be in place which better integrates the data blocking perspective, and the FTC, the agency charged with regulating mobile medical apps.

Recommendation: Whether these vendors of non-certified products are included under the health IT developer definition or the HIN definition (discussed more below), it is our position that they must be governed by ONC's information blocking rules.

Iii & Iv. HINs & HIEs

Pertaining to the definition of exchanges and networks, these terms are not defined in the statute providing ONC significant flexibility to propose definitions. ONC's proposed definitions for HINs and HIEs are fairly broad, especially the HIN category. ONC proposes that an actor would be a HIN if they "determine, oversee, administer, control, or substantially influence policies or agreements that define the access, exchange, technical, or other conditions or requirements that enable or facilitate the access, exchange, or use of EHI between or among two or more unaffiliated individuals or entities." ONC further says an actor would be an HIN if they, "manage, control, or substantially influence any technology or service that enables or facilitates the access, exchange, or use of EHI between or among two or more unaffiliated individuals or entities." ONC clarifies that two parties are affiliated if one has the power to control the other, or if both parties are under the common control or ownership of a common owner. Given how broad this category of actors could be, additional examples of who ONC envisions fitting under these would be helpful. For instance, would a provider who treats a snowbird who shows up in their hospital emergency room be considered a HIN?

Similarly, ONC defines a HIE as an individual or entity that enables access, exchange, or use of EHI primarily between or among a particular class of individuals or entities or for a limited set of purposes. The rule also provides a non-exhaustive list of entities that are HIEs.

In reviewing the proposed definition of a health IT developer, HINs and HIEs, we had questions about how prescription drug monitoring programs (PDMPs) fit into this set of actors. We understand that PDMPs are not certified modules subject to requirements under the certification program. Although they connect to a certified EHR we seek clarification as to whether the ONC's proposed definition therefore excludes them. Similar to our concerns

about the app developer ecosystem, we believe PDMPs also must be governed by the data blocking provisions, whether covered under the health IT developer definition or the HIN or HIE definitions.

Recommendations:

1. **App developers and technology giants who manage the app ecosystem, as well as PDMPs, should be included in either the categories of HIEs and HINs, depending upon the type of action they perform. And, if the definition does not accommodate these entities, ONC should expand these categories of actors to include them; and**
2. **Providers who also meet ONC's definition of a developer, HIN or HIE should only be subjected to the enforcement mechanism related to providers since they are doing so to facilitate patient care.**

C. Definition of EHI

The definition of electronic health information (EHI) is not specifically defined in the statute. The proposed rule defines EHI as electronic protected health information (ePHI) and any other information that is:

- Transmitted by or maintained in electronic media;
- 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 healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual.

Our members are committed to ensuring patients have timely access to their records. However, we are very worried that the EHI definition proposed by ONC is overly broad, exceeds what was intended by Congress, and would be administratively complex to meet. Specifically, Section 4006 of the Cures Act clearly directs the Office for Civil Rights (OCR) in consultation with ONC to help patients understand their HIPAA "right of access." The challenge arises because ONC's proposal for establishing a definition of EHI exceeds what is contained in HIPAA's right of access. Under 45 CFR Section 164.524, the right of access provision in HIPAA says, "an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, except for: (i) Psychotherapy notes; and (ii) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding."

Under ONC's current EHI proposal, providers would need to ensure that data can be ported from systems that are non-certified and that data can be ported even when there is no standard (i.e., pricing information). In this scenario, vendors who do not have certified systems on the CHPL would have no responsibility under the ONC rule to help export this data, placing the burden for ensuring the data portability entirely on the providers. It will be critical that developers offer providers a clear understanding of the data that is being ported. And, as we discuss in greater detail below under the Information Blocking section, exceeding what is required under HIPAA becomes an unduly complex undertaking and will create excessive administrative burden. Further, we address additional comments on EHI export issues in the "Changes to 2015 CEHRT" section.

Recommendation:

1. **Limit EHI data that is contained in a certified product which is part of the legal medical record; and**
2. **Require developers to provide a plain English definition of legal medical record as part of the record export.**

IV. Exceptions to Information Blocking

The Cures Act grants HHS the authority to identify "reasonable and necessary activities" that would not implicate the information blocking provisions. In this proposed rule, ONC identifies seven categories of such activities and provides the corresponding requirements and conditions that would need to be met. We offer comments on exceptions 1 through 4 below.

Exception #1: Patient Harm

ONC proposes to establish an exception to the information blocking provision for practices that are reasonable and necessary to prevent harm to a patient or another person, provided certain conditions are met. CHIME supports ONC's proposal for the first exception related to patient harm. We believe this will help promote information sharing across the care continuum. However, we nonetheless have some practical concerns.

While ONC acknowledges laws like 42 CFR Part 2 require patient consent before sharing, they also state that the exemption cannot be justified just because a patient didn't give consent to share some information such as sensitive data (i.e. Part 2) thus making the record incomplete. Unfortunately, many EHRs cannot segregate sensitive data from other data. CHIME strongly supports aligning Part 2 requirements around sharing sensitive health information with HIPAA rules on less sensitive health information. However, until these policies are aligned and until EHRs are evolved to the point where sensitive data can be easily segmented, providers will experience challenges outside their control related to sharing records containing sensitive health information. We also fail to understand how the information blocking rule supersedes Part 2 rules. Last, we are aware that SAMHSA is planning on releasing new rules around Part 2 shortly and it will be important to review any changes prior to finalizing this exception.

ONC also discusses the concerns related to withholding the sharing of information when there is a risk of misidentifying a patient's EHI. Given CHIME's long-standing support of the need for a patient identification strategy and the importance from both a patient safety and interoperability standpoint of being able to connect the right patient with their records, we strongly support ONC recognizing these concerns. In the absence of a patient identification strategy, we wholeheartedly agree with ONC that accurately matching a patient to their records remains a complex undertaking.

Additionally, ONC says a health IT developer of certified health IT cannot refuse to provide a batch export on the basis that the exported records may contain a misidentified record. And, similarly, a health care provider that identified a particular piece of information had been misattributed to a patient would not be excused from exchanging or providing access to all other EHI about the patient that had not been misattributed. Overall, however, we recognize having access to data in a timely manner is an imperative. Our long-term / post-acute care (LPTAC) members report they are not getting access to consolidated clinical data (CCDs) in a timely manner. One member who reported frustration with receiving timely CCDs, attributed this to the vendor's unwillingness to share data until

"all t's are crossed." The member reported that even when not all the data is needed, the vendor won't send the record along, "until they have the last lab." Clearly the timing of data exchange is critical in the decisions necessary to provide the "right" care. It will be necessary to ensure that all of the players understand the rules around not delaying export based on "what if's."

Recommendations:

1. **CMS and ONC should identify, with providers, a definition of data that is pre-releasable before the CCD is grouped and sent, and vendors should be required to accommodate this.**
2. **Vendors should provide functionality that eases the burden of separating behavioral health notes from the rest of record.**

Exception #2: Promoting the Privacy of EHI

ONC's second exception applies to reasonable and necessary actions that protect the privacy of an individual's EHI, provided certain conditions are met. ONC affirms that any practice to protect the privacy of an individual's EHI must be consistent with applicable laws related to health information privacy, including the HIPAA Privacy Rule as applicable, as well as with other applicable laws and regulations, such as the HITECH Act, 42 CFR Part 2, and state laws. ONC further proposes that an actor would need to satisfy at least one of four proposed sub-exceptions in order to be covered by this exception.

The four sub-exceptions are as follows:

1. **Pre-condition not satisfied:** Not providing access, exchange, or use of EHI when a state or federal law requires that a condition be satisfied before an actor provides access, exchange, or use of EHI, and the condition is not satisfied (proposed in § 171.202(b));
2. **Developer not covered by HIPAA:** Not providing access, exchange, or use of EHI when the actor is a health IT developer of certified health IT that is not covered by the HIPAA Privacy Rule in respect to a practice (proposed in § 171.202(c));
3. **Denying right to access:** A covered entity, or a business associate on behalf of a covered entity, denying an individual's request for access to their electronic PHI under HIPAA; and
4. **Individual's request not to share:** Not providing access, exchange, or use of EHI pursuant to an individual's request, in certain situations.

Our members take seriously their responsibility to safeguard and protect the privacy of patient information with which they have been trusted. Overall, while we appreciate the detailed approach and intention behind this exception, unfortunately our members found exception #2 with the four sub-exceptions to be overly complex, and if adopted as proposed, could create unnecessary administrative complexity and burdens.

Moreover, some members posited that if this proposal is adopted as proposed that it could have unintended consequences. Specifically, they believe this could lead to oversharing of information so as not to invoke information blocking provisions. Conversely, they also would expect some providers to create overly restrictive policies so as not to violate HIPAA rules.

ONC furthermore notes, "the information blocking provision may operate to require that actors provide access, exchange, or use of EHI in situations that HIPAA does not. This is because the

HIPAA Privacy Rule permits, but does not require, covered entities to use and disclose ePHI in most circumstances." We concluded that this alone would be significantly challenging to meet by creating a scenario whereby a provider would have to follow one set of rules for HIPAA (i.e., treatment, payment or healthcare operations) and an entirely different set of rules which could require policies that mandate they share information or risk running afoul of the information blocking provisions. It thus appears to set up a separate regulatory schematic that would have the effect of providers having to navigate a dual and sometimes conflicting privacy paradigm.

Recommendation:

In order to reduce the significant administrative complexity that will ensue if this proposal is finalized as adopted, we request that providers only be required to meet existing requirements under HIPAA. Or, if that is not possible, we urge HHS to amend and align the HIPAA rules.

Sub-exception #1: Precondition not satisfied

ONC created this sub-exception for the purpose of protecting entities who do not exchange or allow access to information when a state or federal law requires that a condition be satisfied before an actor provides access, exchange, or use of EHI, and the condition is not satisfied. ONC provides examples of when sharing information can be restricted for the purpose of meeting this sub-exception:

- Example #1: While HIPAA does not require patient consent to share PHI for treatment, payment or healthcare operations (TPO), some state and federal laws require consent be obtained first (i.e. HIV, mental health, genetic testing).
- Example #2: Part 2 rules require patient consent prior to sharing substance abuse information.
- Example #3: Providers may share info with another provider for quality improvement if they have verified requesting entity has a relationship with the person whose information is being requested.
- Example #4: Patient pays out of pocket and requests data not be shared with their health plan.

Of the four sub-exceptions our members believe the first sub-exception would be the most complicated to implement. The feedback we received from members – several of whom act as privacy officers for their organization – questioned how this sub-exception would work. They asked:

- How will they be expected to meet this sub-exception for patients who pay out of pocket? Managing patients who pay in full for their care requires providers not submit their information to insurance companies and is already very complicated.
- Is this just for Medicare or all patients?
- How will this sub-exception work for patients who opt out of an HIE? Would information blocking provisions apply?
- Why should developers who are not covered by HIPAA be let off the hook when it comes to moving patient information? How can the healthcare system be safeguarded if segments of vendors are not required to follow the same rules?

ONC also says they are considering inclusion of an accommodation in this sub-exception that would recognize an actor's observance of a legal precondition if that actor is required by law to satisfy it in at least one state in which it operates. Our members also had questions about how this would work since HIPAA always requires that they fall back on the most restrictive set of rules for sharing. ONC, however, also says "we would also need to carefully consider how to ensure that before the use of the most stringent restriction is applied in all jurisdictions, the actor has provided all privacy protections afforded by that law across its entire business." They found these two thoughts contradictory and wondered:

- Why aren't existing policies enough to handle this? Why is this needed?
- How will this work with patients who seek care in non-adjoining states, such as in the case of "snowbirds"?
- How would this proposal work with existing HIPAA requirements?
- How will this work for providers who serve as referral clinics to other large providers? For instance, if a provider lives in a state that receives a significant number of non-resident, "seasonal" patients and you multiply this many times, how will providers be expected to manage the multiple permutations of different privacy policies at the state and federal level?
- If acting outside your policies, you could get a sub-exception if you properly document, but you must give patients the chance to share information. Again, how will this work with opt-out states? Will this present conflicts?
- More "restrictive" can depend on the data you are dealing with. How does ONC plan to treat data types that are more restrictive when it involves moving data across state lines?
- Would it be the more restrictive based on where the data is generated?
- How does this proposal intersect with OCR's review of privacy practices under their recent RFI?

ONC also says to qualify for this sub-exception the providers must properly document the rationale. A provider would be required to give patients the chance to consent to share information, and a provider would be prohibited from encouraging patients not to share their information. Our interpretation of this proposal suggests that, while we can share info under HIPAA (TPO), providers would still need to prove they gave patients a choice. Assuming our interpretation is correct, this will create significant administrative burdens and complexity. Further, it would result in a scenario as described earlier that could lead to over- or under-sharing.

Specific questions our members posed for ONC include:

- What is the statutory authority with which EHI is being bestowed, and how is this any different from PHI?
- How is this different from what is already intended under HIPAA and how would this solve issues not already addressed by HIPAA?
- Again, how does this work with existing opt-in versus opt-out policies? Since many states are opt-out, does this conflict with this proposed policy and does it make it harder for an organization to comply?
- Could this deter some vendors who otherwise should get certified to avoid it so as not to invoke information blocking provisions?

ONC also says that an actor must provide the patient with a chance to consent / authorization to share information. And, ONC asks what actions an actor should take within their control to provide an individual with a meaningful opportunity to provide a required consent or authorization, and whether different expectations should arise in the context of a consent versus a HIPAA authorization. We understand and appreciate the intent; seemingly there

shouldn't be new policies that discourage patients from sharing their information. However, we worry that requiring providers to create new policies beyond HIPAA aimed at offering patients a "meaningful" opportunity to consent, erects more challenges than solutions and will create unnecessary administrative burdens and complexity for providers. Providers are already very accustomed to working with HIPAA requirements and this wording creates a confusing and separate set of rules. Further, rather than creating new policies, a better approach would be to have providers leverage any opportunity under HIPAA (i.e., check in) when seeking consent.

Finally, ONC says that qualifying for this sub-exception furthermore requires that a practice must be tailored to the specific privacy risk or interest being addressed and that the practice must be implemented in a consistent and non-discriminatory manner. We believe this goes back to the notice of privacy practices and whether providers are following the rules as intended. Unfortunately, while well intended, our members believe this could lead to an unnecessary complexity, and such a policy is overly prescriptive. Our members continue to report that many patients don't bother to read privacy practices so we fail to see how making things more complicated will change anything for the patient.

Recommendations:

1. **Providers should be allowed to meet the most restrictive policy (i.e., state) when sharing information about patients across any state line;**
2. **ONC should provide more use cases to help providers and others better understand how this pre-condition sub-exception can be met; and**
3. **Changes must be completely aligned with HIPAA and if there are divergences, they must be clearly reconciled. Moreover, there has been speculation that this rule is aimed at making changes to HIPAA. While not explicitly stated, it is unclear how the changes in this rule will affect a provider's ability to comply with both mandates. We strongly recommend the Administration clearly delineate their expectations and that the administrative burden on having to meet two sets of rules be carefully assessed.**

Sub-exception 2: Health IT developer of certified health IT not covered by HIPAA

This sub-exception addresses circumstances where a health IT developer of certified health IT offers a health IT product or service not regulated by the HIPAA Privacy Rule that is subject of the information blocking provision. ONC developed this sub-exception to address non-covered actors engaged in reasonable and necessary privacy-protective practices that interfere with the access, exchange, or use of EHI.

We interpreted this sub-exception to represent a fairly narrow set of developers, such as those vendors who are certified for a very particular function like a reminder system. However, as ONC notes this would apply to direct-to-consumer health IT products, which is a growing segment of the healthcare technology sector. Some members felt this sub-exception could be helpful for those developing their own health IT tools, which are outside of the EHR.

Recommendation:

We request clarification and more examples to ensure we understand the intent of sub-exception #2, including whether this is intended to apply to population health vendors or any other narrow segment of healthcare technology sector.

Sub-exception 3: Denial of an individual's request for their ePHI

ONC writes that it crafted this sub-exception to address situations where it is reasonable for an actor to deny access to an individual, consistent with denials permitted under the HIPAA Privacy Rule. While on the surface our members thought the concept of sub-exception #3 made sense, they also had operational concerns like those articulated under sub-exception #1 in terms of how these two carve-outs would work in practice. ONC says they believe this exception would avoid a potential conflict between the HIPAA Privacy Rule and the information blocking provision. As noted earlier, we have several questions about how this would work in reality. Members were concerned there would be too much burden on providers to demonstrate the right type and amount of information was shared.

Recommendation:

Like sub-exception #1, our members have several operational concerns and request that ONC offer more details around how this sub-exception would work in practice and how providers can avoid challenges complying with HIPAA.

Sub-exception 4: Respecting an individual's request not to share information

The fourth exception is intended to further assure actors that they can respect individuals' privacy choices without engaging in information blocking, including if an individual does not wish to provide access, exchange, or use of their EHI. ONC also states this sub-exception will promote public confidence in the health IT infrastructure by respecting patients' preference about how and under what circumstances their EHI will be accessed. To meet these goals, the proposed sub-exception #4 in certain circumstances, would permit an actor not to provide access, exchange, or use of EHI if an individual has specifically requested that the actor not do so. Members again had questions about ensuring there are no conflicts with what is permitted under HIPAA's TPO rules, as well as questions about how this would work with opt-in / -out policies. Some members wonder how this is any different from what is allowed under HIPAA. Is the primary difference that this extends to EHI, which is more expansive than ePHI?

Recommendation:

ONC must clearly articulate how this proposal differs from what is allowed under HIPAA. In its response to this recommendation, we request that ONC identify whether the primary difference is that this extends to EHI, which is more expansive than PHI.

Exception #3: Promoting Security of EHI

ONC's third proposed exception would allow actors to engage in practices that are reasonable and necessary to promote the security of EHI, subject to certain conditions. The rule specifies the conditions must be met to qualify for this exception, including in the following areas:

- The practice must be directly related to safeguarding the confidentiality, integrity, and availability of EHI.
- The practice must be tailored to the specific security risk being addressed.
- Practice must be implemented in a consistent and non-discriminatory manner.
- Practices that implement an organizational security policy.

- Practices that do not implement an organizational security policy (i.e. when novel threats arise).

Our members are pleased to see the attention to security and the acknowledgement of cybersecurity threats faced by our industry. ONC writes in the rule, "Robust security protections are critical to promoting patients' and other stakeholders' trust and confidence that EHI will be collected, used, and shared in a manner that protects individuals' privacy and complies with applicable legal requirements. Public confidence in the security of their EHI has been challenged, however, by the growing incidence of cyber-attacks in the health care sector. More than ever, health care providers, health IT developers, HIEs and HINs must be vigilant to mitigate security risks and implement appropriate safeguards to secure the EHI they collect, maintain, access, use, and exchange."

Recommendations:

1. **Security concerns must be more thoroughly probed. In considering ONC's proposal under exception #4, our chief concerns lie with APIs and how providers are expected to know what kind of risks they are undertaking when connecting with them. We detail the genesis of our concerns around API security in the "Conditions and Maintenance of Certification" section of our letter; and**
2. **The Cures Act requires ONC in consult with OCR to issue guidance on common "security barriers" that prevent the trusted exchange of EHI. To date, we have not seen this guidance and request an update from ONC on the expected timeframe for this guidance.**

Exception #4: Recovering Costs Reasonably Incurred

ONC says they interpret the definition of information blocking to include any fee that is likely to interfere with the access, exchange, or use of EHI. However, ONC also notes, "this interpretation may be broader than necessary to address genuine information blocking concerns and could have unintended consequences on innovation and competition."

Exception #4 would permit the recovery of certain costs reasonably incurred to provide access, exchange, or use of EHI, subject to strict conditions to prevent its potential misuse. ONC says they are concerned that a broad or insufficiently tailored exception for the recovery of costs could protect rent-seeking, opportunistic fees, and exclusionary practices that interfere with the access, exchange, and use of EHI. The proposed rule states that the method by which an actor recovers its costs must not be based on the sales, profit, revenue, or other value derived from the access to, exchange of, or use of EHI, including the secondary use of such information, that exceeds the actor's reasonable costs for providing access, exchange, or use of EHI.

ONC emphasizes that such revenue-sharing or profit-sharing arrangements would only be acceptable and covered by the exception if such arrangements are designed to provide an alternative way to recover the costs reasonably incurred for providing services. And, ONC specifically calls for excluding certain costs regardless of this exception, which include: costs due to non-standard design or implementation choices; subjective or speculative costs; fees prohibited under the HIPAA Privacy Rule; individual electronic access; and export and portability of EHI maintained in EHR systems.

We perceive ONC is taking a narrow and tailored approach in articulating what would qualify for this exception. As a result, we would expect, few instances where fees would be permitted surrounding the access or exchange of data without involving a violation of data blocking. We appreciate that ONC is pushing the industry not to use costs to restrict the flow of information. In approaching this exception ONC does not dictate any cost structure per se,

however, they do set criteria around what is prohibited. While we support the notion of prohibiting costs from being a limiting factor in impeding the flow of patient data, we have issues we hope ONC will consider.

- **Providers who did not qualify for HITECH monies:** We strongly believe that additional consideration is needed to accommodate providers who did not qualify for Promoting Interoperability (formerly referred to as Meaningful Use) incentives. While several of the clinicians named in ONC's proposed definition of provider were in fact eligible for incentives, the institutions where they work – such as nursing homes, home health, skilled nursing facilities and mental health providers – were not. As such, many of these entities do not have certified technology. The costs to come into compliance for the purposes of information blocking is expected to be very significant. One of our PAC members reported that they asked their vendor who is not certified to provide audit logs and the vendor didn't have this information. We question the fairness of requiring providers who do not have certified systems or even ones that do but did not qualify for HITECH monies from having to be subject to these requirements on the same timeline as those who did. Exceptions should be made at least in the near term for these providers.

- **Cost Structures:** ONC says under exception #4 that it doesn't mean an actor must apply the same prices or price terms for all persons or classes of persons, however, to qualify for the exception the costs must be reasonable. What this appears to propose is that an actor cannot recover total costs, which we believe is reasonable. We encourage ONC to clarify this point.

Recommendations:

2. **Account for providers who did not qualify for EHR incentives and do not have certified EHRs by:**
    a. **Giving more time to comply with information blocking provisions;**
    b. **Offering additional education and outreach to ensure they are in compliance; and**
    c. **Offering safe harbors for providers who do not have certified products.**

V. Patient Matching RFI

Included in the ONC and CMS rules are complementary requests for information regarding patient matching. We are delighted to see the Administration focusing on such a critical issue. CHIME has long contended, and, in fact, has been a trail blazer in championing this issue. The ability to uniquely connect a patient to their medical record is paramount for both interoperability and patient safety reasons. We would note that the term patient matching is often used interchangeably with the term patient identification. We believe that patient identification – meaning the ability to uniquely and accurately match a patient to their record – as opposed to a referential matching algorithm is the right solution. Without accurately connecting a patient to their data, patient safety and interoperability issues will persist.

Understanding, however, that the Administration is prohibited by Congress from spending time or resources on adopting a standard to uniquely identify patients, we are very pleased the Administration is exercising the authority granted by Congress under the previous two appropriations reports which contain language encouraging the Department to identify industry-led solutions to improve patient matching. Given our long-standing interest surrounding unique patient identification, we are pleased to offer our comments these topics.

Healthcare organizations and agencies, such as the Department of Defense (DOD) and the National Institute of Standards and Technology (NIST) consider accurate patient matching a combination of people, process, and technology. This information is then entered into electronic fields using standard, unique identifier conventions. For example, NIST recommends name followed by name modifier (e.g., Jr., Sr., III), date with month written in first 3 or 4 letters (e.g., Jan—). Other suggestions include zip code, address, and historical addresses. Standards for naming conventions and processes in support of usability such as these combined with safety guidelines and training could be leveraged.

CMS

CMS seeks input on how the Agency could leverage its program authority to provide support to those working to improve patient matching. CMS includes extensive discussion of the benefits and concerns around patient matching. CMS writes that patient matching can be less precise than a unique patient identifier (UPI) due to the reliance on demographic attributes (such as name and date of birth) which are not unique traits to a particular patient; further, patient matching is often dependent on manual data entry and data maintained in varying formats. Matching mistakes can contribute to adverse events, compromised safety and privacy, and increased healthcare costs. Recognizing Congress' intent regarding patient matching and some stakeholder comments stating that a patient matching solution would accomplish the goals of a UPI, CMS' patient matching RFI focuses on ways they can continue to facilitate private sector efforts on a workable and scalable patient matching strategy so that the lack of a specific UPI does not impede the free flow of information.

CMS specifically requests input on whether they should expand the use of the Medicare ID card by requiring a CMS-wide identifier which is used for all beneficiaries and enrollees in healthcare programs under CMS administration and authority, specifically by requiring any or all of the following: that Medicare Advantage (MA) organizations, Part D prescription drug plan sponsors, entities offering cost plans, and other Medicare health plans use the Medicare ID in their plan administration; State Medicaid and Children's Health Insurance Plan (CHIP) agencies in their fee for service (FFS) or managed care programs; Medicare ID for dual eligible individuals; and qualified health plan (QHP) issuers in federally facilitated exchanges (FFEs) use the Medicare ID for their enrollees in the administration of their plans. The Medicare Beneficiary Identifier (MBI) replaced the use of the Social Security Number beginning in 2018 (now referred to as the Medicare ID card). CHIME believes the idea to expand use of the Medicare ID card holds merit and we encourage CMS to continue exploring this approach. Our members have deduced that it would not be hard for them to have to track this ID since they already track numerous patient IDs issued by multiple payers for patients. According to a RAND study on the patient identity issue, the savings from implementing a unique ID amounts to $77 billion a year.[2] Therefore, the savings from implementing such a policy would be significant.

As the agency explores patient matching, while not specifically called out in the RFI, biometrics have been discussed as a possible option. We are aware that NIST recently released a standard for the use of biometrics.[3] If a biometric is ultimately adopted it must work in a variety of healthcare settings. For instance, one member noted that they use retina scans for patients who cannot get their date of birth correct. That said, while we believe biometrics have an important place and hold much promise, there are nonetheless limitations, including:

[2] https://www.rand.org/pubs/monographs/MG753.html
[3] https://www.nist.gov/programs-projects/biometrics

- **Variability among vendors:** While hard to replicate a biometric image, there can be variability between vendors. Most readers don't store the actual image, just specific points of the image. Biometrics are reading an image and taking and converting points into a hash. For instance, in the case of a fingerprint, different readers will come up with different readings and there is no way to reengineer the hash back to the finger print so this becomes another number in essence. However, if you had the hash and the actual patient ID (i.e. SSN), the combination of the two is virtually impossible to replicate and is virtually unique.
- **Costs**: Implementing biometrics is costly, especially for providers regardless of their size.
- **Its use may not work well in all settings of care:** There are situations when you need to identify a patient in certain settings of care prior to their arrival, such as in the post-acute space, therefore, without the patient actually being present, use of a biometric may be impractical.
- **There are potential risks with EHRs and these apps.** The list could include entering information into the wrong patient record (having multiple patient records open, side by side, or overlaying patient records); untangling (i.e., separating) co-mingled patient information; mistakenly creating duplicate charts; and assigning a test to the wrong patient.
- **Pediatrics:** In January 2019, the Joint Commission added a new required reporting element of performance[4] to align with NPSGF 01.01.01[5], aimed at patient identification, and recommends using distinct methods for identifying newborns in hospitals, such as mother's first and last name plus gender. CMS also requested input on whether they should require Medicare FFS, MA Plans, Medicaid FFS, Medicaid managed care plans, CHIP FFS, CHIP managed care entities, and QHP issuers in the Federally Facilitated Exchange (FFE) to use either a patient matching algorithm with a proven success rate of a certain percentage. Other requirements included were that the algorithm and real-world processes associated with the algorithm used are validated by HHS or a third party, or a particular patient matching software solution with a proven success rate of a certain percentage validated by HHS or a third party. We believe these ideas have merit, especially if expanding the Medicare ID is not feasible and considering our below comments concerning certification. As we describe in the Maintenance of Certification section of our letter, we believe vendors should be required to share their patient matching rate with providers in order to meet the MOC.

Additionally, CMS requests feedback on whether the agency should support connecting EHRs to other complementary verifying data sources for identity proofing. And, they ask what potential data source should be considered, as well as, the possible restrictions or limitations to accessing such information. If CMS is referencing whether providers should have access to CMS claims data, then the answer is a resounding yes as this could improve patient matching. NIST recommends standardizing the display of patient identifiers across various systems, from the registration system through to the EHR. Human factors engineers recommend that information be presented consistently and predictably. For example, ordering patient information the same way (i.e., "LAST NAME," "First Name," and "Middle Initial"). CMS can support this in recognizing the key risk areas of EMR design and advancing these standards by requiring:

1. Information critical to patient identification is consistently displayed in a reserved area to avoid wrong patient errors;

[4] https://www.jointcommission.org/assets/1/18/R3_17_Newborn_identification_6_22_18_FINAL.pdf and
[5] https://jntcm.ae-admin.com/assets/1/6/NPSG_2019_Presentation_-_FINAL.pdf

2. Cues/alerts are provided to reduce the risk of entering information and writing orders in the wrong patient's chart; and
3. Supporting efficient and easy identification of inaccurate, outdated, or inappropriate items in lists of grouped information by having information presented clearly and in a well-organized manner. Information required to accurately identify the patient is clearly displayed on the electronic display of system screens.

Finally, regarding the use of patient-generated data to compliment patient matching efforts, another topic for which CMS seeks input, many of our members store this data in their EHRs today. However, our members noted significant work remains before this could be used to match patients. For example, the validity of data continues to be an issue, since data coming in via patient portals often must be revalidated.

Recommendations to CMS:

1. **Best practice guidelines should include the use of a standardized process for patient identification and capturing patient information no matter where registration occurs;**
2. **We encourage CMS to continue exploring the possibility of expanding the use of the Medicare ID;**
3. **CMS should work with ONC to ensure that vendors as part of their Maintenance of Certification are required to share their patient matching rates and other related information (as discussed in greater detail in that section of our letter);**
4. **If a biometric is ultimately adopted, it must work in a variety of healthcare settings; and**
5. **CMS should make claims data readily available in a timely manner to providers through a FHIR-based API; doing so will help providers better match patients.**

ONC

ONC writes that patient matching is a critical component to interoperability and the nation's health information technology infrastructure. In fact, ONC cited a CHIME survey[6] where one in five providers named lack of an appropriate patient matching strategy as the primary reason for inadvertent illness or injury. ONC stated that it considers this a quality of care and patient safety issue, and requested input on creative, innovative, and effective approaches to patient matching within and across providers.

ONC suggests that patient matching may be defined as the linking of one patient's data within and across healthcare providers to obtain a comprehensive and longitudinal view of that patient's health care. At a minimum, this is accomplished by linking multiple demographic data fields such as name, birth date, sex, phone number and address. ONC specifically asks about the use of certain pieces of demographic data like address and phone number. Some of our members have found the use of phone numbers to be helpful as people tend to keep them for a long time. Addresses, on the other hand, can change often, which can present issues like identity theft (i.e., bills going to an apartment where you previously lived). However, when the address field is standardized – particularly when applying the U.S. Postal Service Standard to the address, matching rates improve. Many organizations—including the Bipartisan Policy Center and ONC contractor Audacious Inquiry—have recommended the standardization of data used for matching, however the effects of standardization have not yet been tested.

[6] https://chimecentral.org/wp-content/uploads/2014/11/Summary_of_CHIME_Survey_on_Patient_Data.pdf

In an article published in March of this year in the *Journal of the American Medical Informatics Association (JAMIA)*[7], the Pew Charitable Trust collaborated with Indiana University to test whether standardizing demographic fields (including address, phone number, name, and others) yields improvements. They found through their research that its use increased match rates by approximately 2-3 percent. To conduct the research, Indiana University ran a matching algorithm across four different databases where the true matches were already known, then standardized the data and re-ran the algorithm to determine whether standardization generated better matching results. We support ONC's proposal to include address among the demographic data elements proposed in the U.S. Core Data for Interoperability (USCDI). ONC could build on the addition of address to the USCDI by specifying the use of the U.S. Postal Service standard for address.

We believe it would also be beneficial for ONC to add other regularly collected data elements—such as email address—to the USCDI. ONC currently requires address, name, birth date, phone number, and sex for matching. However, health records contain other demographic data routinely collected—such as email address and health insurance policy ID. For example, a recent study found that, in 2014, 54 percent of patient records contain email address. As email is increasingly captured, it should be considered for use in matching. ONC should work with the industry and experts to identify additional demographic data to add to the USCDI, such as email address.

It's also worth noting that the Sequoia has studied patient matching.[8] They developed a framework for patient identity management in conjunction with the Care Connectivity Consortium (CCC) and they also studied the integrity of data. They note, "Resolution of patient identity issues are more daunting when they cross organizational lines. Such issues often involve six or more organizations (the two health information organizations, their two vendors, and often an intermediary such as a health information organization and their vendor). In such an environment, even mundane items such as scheduling cross-organizational working sessions often introduce days and weeks of delay in resolving each issue due to lack of availability of key personnel." They also included data on matching from Intermountain Health which found that in their health system comprised of 22 hospitals, 1,400 employed doctors, 185 clinics, and health plans they were able to improve patient matching from 10% to 95%. Specifically, Sequoia reports that with "demographics-based patient matching" Intermountain was able to show, "with proper data quality control and algorithmic adjustment, demographic-based patient matching can achieve mathematically promising matching rates." Their report details the patient attributes with the highest success rates included first and last names, gender, date of birth, postal code and primary phone number.

AHIMA has also studied this topic and has identified several best practices providers can employ around patient identity:[9]

- Two-factor which could include verifying an address
- Verbally verifying a patient's information by making them re-state it (as opposed to just saying yes or no)
- Presenting a driver's license for applicable populations
- Having patients read wrist bands or verify information on a computer screen
- Taking photos of a patient
- Using patient registration kiosks

[7] https://academic.oup.com/jamia/article-abstract/26/5/447/5372371
[8] https://sequoiaproject.org/resources/patient-matching/
[9] http://bok.ahima.org/doc?oid=302514#.XKtrwPZFxPY

Finally, our members report that they must often rely on HIEs and vendors for matching. This practice comes with its own set of challenges. For example, some HIEs will not divulge their match rate to providers. Further, there is no certification criteria or certification program that oversees reporting of match rates. Therefore, providers are wholly dependent on the other entities to accurately report their match rate. More could be done to improve transparency and accountability, such as through certification and information blocking.

Recommendations to ONC:

1. **Add patient matching to the certification requirements that vendors must meet. At a minimum, vendors should be required to attest to their matching rate;**
2. **Make it a violation under data blocking not to share a patient matching rate;**
3. **Support the standardization of some demographic data, particularly applying the U.S. Postal Service Standard to address;**
4. **Advance the addition of other regularly collected data elements—such as email address—to the USCDI; and**
5. **Add the Medicare ID number to the USCDI.**

VI. Provider Directories & Contact information

The Cures Act emphasizes the importance of making provider digital contact information available through a common directory. The CMS proposed rule proposes to increase the number of clinicians with valid and current digital contact information available through the National Plan and Provider Enumeration System (NPPES). CMS proposes to publicly identify those clinicians who have not submitted digital contact information in NPPES. Our members are often wrestling with multiple payer directories; therefore, they believe having a single directory could help reduce regulatory burdens. They cited, however, one notable exception: Direct Addresses are too complicated for some members to manage. In operationalizing this requirement, our members have several questions about how CMS' proposal would work in practice. These include:

- **When clinicians have multiple Direct Addresses:** Members report that many clinicians are covered by multiple addresses, making things very complicated to manage. For example clinicians working in rural areas and providers that work in multiple EHRs may have multiple addresses. A hospital might have 30 Direct Addresses and then hundreds for a department. How would addresses be required to be entered into NPPES? Would it be dictated by location? What if a multi-location clinic only has one address; would each clinic be required to register? Would the clinic address be pegged to a Type II NPI rather than a Type I or both?
- **Accessing Direct Addresses:** Another challenge reported by our members is getting access to Direct Addresses. We have several members who have had trouble accessing Direct Addresses via an EHR vendor. One member called a large vendor to get these and was referred to one of the vendor's attorneys who incorrectly notified our member that this was a HIPAA violation.
- **Workflow issues:** Some of the challenges that could be created by this new requirement could manifest themselves in the form of workflow challenges, and thus education will be important.
- **Exchanging data:** Members reported challenges with exchanging data outside of some vendor products. For instance, one vendor told a member they needed XYZ+ product rather than just XYZ in order to

communicate outside the product, a situation that impedes interoperability and unnecessarily increases costs for providers.

CMS also seeks feedback on additional possible enforcement authorities to ensure that individuals and facilities make their digital contact information publicly available through NPPES. When CMS initially required the NPI registration requirements, there was tremendous confusion for providers under requirements for enumeration (i.e. Type I vs Type II). In order to avoid this confusion and unnecessarily penalize providers, prior to engaging in any enforcement activities, providers must be properly educated on these new requirements and they must be sufficiently clear.

Recommendations: CMS should:

1. **Work with providers, vendors and other affected stakeholders to ensure use cases and directions for updating NPPES work from an operational standpoint;**
2. **Engage in a significant education campaign around updating the NPPES with Direct Addresses and other digital endpoints once this process is fully articulated; and**
3. **Consider rolling this out gradually or using a phased approach. Doing so would allow CMS to work with stakeholders to address emergent issues before widespread requirements are in place.**

VII. Medicare COP: Admission, Discharge, Transfer

CMS developed provisions of this rule to further expand the Agency's requirements for interoperability within the hospital and critical access hospital (CAH) Conditions of Participation (CoPs) by focusing on electronic patient event notifications. Specifically, CMS proposes to require Medicare-participating hospitals (including short-term acute care hospitals, long-term care hospitals (LTCHs), rehabilitation hospitals, psychiatric hospitals, children's hospitals, and cancer hospitals) and critical access hospitals (CAHs) to send electronic event notifications. Hospitals would be required to send electronic patient event notifications of a patient's admission, discharge, and/or transfer to another healthcare facility or to another community provider. Hospitals would have to convey, at a minimum, the patient's basic personal or demographic information, as well as the name of the sending institution, treating practitioner's name, and, if not prohibited by other applicable law, the diagnosis.

In reviewing CMS' proposal, we agree with the intent and spirit of what the agency is aiming to achieve by facilitating better information hand-offs and exchange between providers when their patients are admitted, discharged, and transferred. We also agree that much of what CMS aims to accomplish can happen. We wish to underscore the significance of making this a condition of participation, since doing so could jeopardize a provider's entire Medicare reimbursement. It seems premature to do this, especially given the challenges we outline below. Therefore, we strongly recommend that prior to making it a Medicare Condition of Participation (CoP), the process by which this can occur needs to be adequately resolved to address the concerns and questions we posit below.

Regarding the implementation timeline, we urge CMS to provide a voluntary, phase-in period of no less than three years. A flexible phase-in period is essential for accommodating the complexity of issues individual providers will need to work through. In reviewing the details of this proposal, we identified the following significant implementation challenges and outstanding questions:

- **Lack of a certification standard to support event notification:** As CMS noted in the rule, there is no criterion under the ONC Health IT Certification Program that certifies health IT to create and send electronic

patient event notifications. Also, we do not agree with CMS' assumption that certified EHRs will be able to handle ADTs just because these systems are currently able to handle other Health Level 7 (HL7) functionality like immunization registries and lab results. While it's true the HL 7 ADT is widely adopted, the challenge is the HL7 protocol cannot be sent through Direct Messaging, Care Equality and other exchanges used for the CCD/CCDA discharge. We recommend the agency conduct further analysis of the existing functionalities and how these align with the proposed future requirements.

Additionally, hospitals who are not part of an HIE that can manage and direct the flow of the ADT to the appropriate provider would have to custom develop and maintain this functionality on their own. It would create a significant burden for these hospitals to develop and maintain the workflow and functionality on their own to satisfy the proposed requirement to send ADT messages to other providers. This would require new considerations for audit evidence and supporting documentation such as an HL7 message and some configuration screen shots.

- **Admission:** CMS calls for providers, upon admission, to send alerts to other clinicians / providers with whom the patient has an established relationship. Many of our members' patients, however, do not have a primary care provider, and the proposed rule does not adequately address this situation.

- **Patient matching and safety issues:** Our members worry that CMS is requesting that providers only send a few pieces of data, which we feel is insufficient to match patients. Within each data segment there are hundreds of pieces of data that can be sent and with CMS requesting only a few, we have serious concerns about the ability to match patients on the receiving end. For example, if all you have is the patient name, diagnosis, name of treating provider and sending institution there will be challenges matching patients correctly.

- **Compliance Burdens:** CMS believes this proposal would impose minimal additional costs on hospitals and the cost would largely be limited to the one-time cost for initial implementation of the notification system, to revision of policies and procedures as they relate to discharge planning; and for communicating these changes to affected staff. We believe CMS has significantly underestimated the complexity of meeting this mandate, and we do not agree with the agency's estimation that this should require little effort and be a one-time cost.

- **Identifying receiving providers / clinicians:** CMS says a hospital would only need to send notifications to those practitioners for whom the hospital has reasonable certainty of receipt of notifications. Again, while we appreciate the intention behind this, it would seem nearly impossible for providers to identify which providers need to receive alerts without some sort of system or registry in place that correctly identifies the patient's primary care provider. As part of the review of this requirement, we ask CMS to consider the following challenges and situations associated with identifying the clinicians / providers who should receive a patient's information under this proposal.

  CMS calls for providers, upon admission, to send alerts to other clinicians / providers with whom the patient has an established relationship. As we previously noted, many of our members' patients do not have a primary care provider. We envision that without such a registry, hospitals will face pushback from clinicians saying this is not my patient. Further, for patients who visit a large group practice, it is common for them to see multiple clinicians within the practice. In this case who should be notified? We are very concerned about the burden on both sending and receiving providers in the absence of a clear process for naming a

primary care / lead clinician (some patients as well may identify their primary physicians as being a specialist such as a cardiologist). In other instances, Medicare may have assigned a patient to a certain clinician, but the patient may not consider that doctor to be their primary care provider.

We have significant questions and concerns as to how hospitals can be expected to identify providers who have a reasonable certainty of receipt of notifications. One member told us that half the doctors in his rural community can't accept an HL7 message. Another member expressed concern that small providers will not have the ability to accept this information. As one member noted, "It's one thing to ship this all out the door but it must land in a place that makes sense. For care management teams to know they must have a safer place to land."

We are also unclear how CMS anticipates handling scenarios where a provider belongs to multiple HIEs. How would a provider know if the receiving clinician received the patient's information? And, how does CMS envision scenarios when a clinician works at multiple hospitals – will the clinician get feeds from all three? We also are unclear how a sending provider knows who is connected via an HIE.

Additionally, while we are in strong favor of phasing out faxing, the reality is that most clinicians still rely very heavily on the fax machine. Moving beyond faxing requires removal of systemic barriers. For example, our rural members report that the Indian Health Services still relies heavily on faxing, which has indirect implications for the providers that must comply with CMS' rule. One member noted that their facility is the only tertiary facility in town. Additionally, while their facility has an EHR from large, well-known vendors, they still experience challenges receiving notices about their patients.

- **Technical capability:** In the proposal CMS intends to apply this requirement only to those hospitals with the "technical capacity" to generate ADT information. We appreciate this parameter is intended to accommodate Medicare- and Medicaid-participating hospitals that have not been eligible for past programs promoting adoption of EHR systems. We seek clarification on CMS' intent in determining the universe of hospitals that will need to comply. Questions raised by our members include:
    - Does not buying or not implementing an interface because it's too costly mean you don't have the capacity?
    - The basic demographic HL7 ADT segment does not have a true diagnosis. It also has many segments with dozens of data elements which a hospital could send with hundreds more data elements than CMS has proposed. What is the expectation?
    - How could providers remain in compliance with HIPAA if they are sharing information that is not necessary for downstream providers?

- **Diagnosis:** CMS requires that diagnosis be included in the information shared. However, oftentimes this information is not available upon admission. For most of our members the final diagnosis is not present until after discharge. Receiving providers understand hospitals are sending a presenting symptom, however it is not considered a true diagnosis.

- **Discharge:** In the PI program, hospitals have been focusing on the exchange of a robust set of clinical data through exchange of CCDA documents through Direct Messages. This proposal would introduce a completely new mechanism that does not align with work currently underway to meet the 2019 program requirements. It seems hospitals would have to shift focus to this new requirement in order to satisfy the change in the Medicare Conditions of Participation.

CMS says it is not their intention to disrupt workflow at discharge and that they do not want to limit providers if they have a better or more robust way to do the notifications. We believe that in order to ensure current processes are not disrupted. CMS should permit those providers who are already doing discharge notifications in a more robust manner be permitted to continue. To this end, CHIME seeks clarity from CMS on the following issues:

- If a provider is sending a CCDA to another provider at discharge, would the sending provider be required to duplicate their work by creating HL7 ADT transactions as well?
- Many members have invested a lot of time, energy and resources to set up Direct Messages and they already have directories to send and receive CCDs. Is it CMS' expectation that providers set up directories for HL7 for ADT messages?

- **Demonstrating information exchange:** In meeting this requirement, affected hospitals would need to demonstrate they send notifications directly, or through an intermediary that facilitates exchange of health information. How will hospitals be expected to demonstrate they are sending the notifications either directly or through a health information exchange?

- The Strategic Health Information Exchange Collaborative (SHIEC) recently announced a program where its members will be able to receive ADT notifications from other connected members. Carequality has just announced the formation of a "push" notification workgroup. It is expected that CommonWell will also develop this capability soon. The proposed rule does not clearly specify the deadline by which CMS expects hospitals to be compliant with this requirement. Further, for hospitals that are not part of these exchange organizations, the proposal would impose significant burdens. These hospitals would have to develop and maintain the workflow and functionality on their own to satisfy the proposed requirement to transmit ADT messages to other providers.

- **Measuring success**: We request that CMS elaborate on what the Agency envisions as success under this policy. In doing so, we recommend against measuring the number of ADTs sent as that metric. We believe a deeper understanding of the Agency's measure of "success" will assist providers and stakeholders in focusing and aligning to realize the desired outcomes.

Recommendations: We recommend CMS:

1. **Adopt the ADT proposal ideally only after there is a certification requirement specifically designed for ADTs and after the above outlined challenges have been addressed. At the very least, we recommend the effective date be set no sooner than three years from the time the rule is finalized;**
2. **Identify solutions to minimize the administrative burden the ADT proposal will place on providers, particularly small and rural providers; and**
3. **If CMS finalizes its ADT discharge requirement as proposed, they should permit providers to use CCDs to meet the requirement.**

VIII. Advancing Interoperability in Innovation Models

CMS believes the Center for Medicare and Medicaid Innovation (CMMI) models provide an important lever to advance progress toward interoperability. The Agency writes that these models offer unique opportunities to engage with health care providers and other entities in innovative ways and to test concepts that can accelerate

change in the U.S. healthcare system, including to promote interoperability. CMS seeks feedback on interoperability within CMMI models for integration into new models. CMS identified three general principles it could apply to promote interoperability in innovative models. These are:

1. Provide patients access to their own electronic health information;
2. Promote trusted health information exchange; and
3. Adopt leading health IT standards and pilot emerging standards.

CMS goes on to write that as part of the design and testing of innovative payment and service delivery models, CMMI anticipates taking on a leadership role in developing new or less mature FHIR and supporting more innovative interventions undertaken by states, whenever possible.

We refer CMS to our discussion in the Section below on the Care Continuum for our thoughts on this.

IX. Health IT and Support for the Care Continuum

ONC's modifications to the CEHRT 2015 Edition were intended to make it more open and accessible to more types of health IT, including health IT that supports various care and practice settings beyond those included in the EHR Incentive Programs. ONC's goal with this program is to continue to support the advancement of interoperable health IT and to promote health IT functionality in care and practice settings across the care continuum. CHIME appreciates the Administration's attention to fostering interoperability across the care continuum and CMS' attention to fostering information sharing and care delivery across all settings of care like long-term, PAC and behavioral health, rather than just to those settings that were eligible for HITECH monies.

With regard to health IT in medical specialties, ONC refers to its previous statements that it did not intend to develop and issue separate regulatory certification "paths" or "tracks" for particular care or practice settings (e.g., a "long-term and post-acute care (LTPAC) certification") because it would be difficult to independently construct such "paths" or "tracks" in a manner that would align with other relevant programs and specific stakeholder needs. Instead, ONC writes that it has explored how it might work with the industry and with specialty organizations to collaboratively advance health IT that supports medical specialties and sites of service. In this proposed rule, ONC discusses insights it gained from stakeholders regarding the challenges they face. ONC states that it believes the Cures Act closely aligns with ONC's ongoing collaborative efforts with both federal partners and stakeholders within the healthcare and health IT community to encourage and support the advancement of health IT for a wide range of clinical settings.

ONC believes it needs to explore ways to advance health IT across the care continuum to support efforts to fight the opioid epidemic and is seeking feedback 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. Using this feedback, ONC plans to improve access to data from disparate sources and help ensure that key data is consistently available to the right person, at the right place, and at the right time across the care continuum. ONC feels progress on this goal can be made by advancing technical standards for exchanging health information that forms an essential foundation for interoperability. CHIME strongly supports this work. Our own Opioid Task Force is committed to finding ways to bend the curve of addiction by leveraging technology.

From an interoperability standpoint, things like opioid databases are improving, but efficient workflow remains a major challenge. Clinicians need to exit the EHR to locate what medications a patient is on and it takes 8-9 minutes to process. Further, better coordination and collaboration is needed with those involved with the treatment of substance abuse, because not all information about these patients is available to clinicians involved in the patient's care.

We also need to eliminate the confusion generated between what was prescribed during the patient's stay in acute settings, and what medications need to stop or continue as they transition from acute care and back to home again. When a patient with a chronic condition is discharged to PAC and then home, it is very difficult to reconcile what medications the patient needs to continue based on prior (home) medication history that may have started with primary care, or started new with an emergent condition that put them in the acute setting, and then must be reconciled when transferred to a post-acute stay. Often the patient or the family is the source of current medication information, which can easily be miscommunicated. Some PAC providers have begun staffing using internal medicine specialists to help deliver the more complex care that these patients are now requiring. Timely and efficient reconcilement of medication history with new medications is vital as a patient recovers. Without it, patient safety is at stake and the cost of delivering care will continue to rise.

In discussing the challenges we see in our industry around fostering information sharing across the care continuum, in addition to the challenges we have already discussed around patient identification, one issue repeatedly rose to the top: the capability of the receiving system to be able to consume data. **We are very concerned that there has been too much focus on the exporting of patient data and little emphasis on the ability for a system to ingest data. We strongly urge ONC and CMS to make this a priority, as we discuss later in our letter.**

Opportunities for Improvement

Vendors are inadequately using the information that is received and parlaying it into meaningful data for providers to foster better treatment. Providers continue to struggle with significant workflow issues related to data received and the manual effort it takes for the clinician to find and locate the information. This presents a burden on the entire healthcare system and contributes to a growing issue of clinician burnout. To quote one member, "Sharing information is good, but if you can't use it then it's just noise." We believe public policy and vendor development must pivot from being exclusively focused on export capabilities to homing in on how importing data can be best supported to foster semantic interoperability. Today the capability still lies largely with EHRs receiving CCDs. EHRs can receive CCDs which are typically filed in a "miscellaneous tab" and does not foster interoperability. While this is better than clinicians having to hunt around for a paper chart, more seamless access to data is needed. As one member put it, "we need to move beyond problem list, medications, and allergies and start to parse CCDs into consumable patient data at the point of care. If new standards aimed at improving interoperability are being required, the ability to appropriately ingest timely and useable information must be considered."

CHIME furthermore appreciates CMS' ongoing work to advance interoperability to improve care coordination, discharge planning, and timely transfer of essential health information for patients. CHIME members are expertly familiar with what is at stake and the complexity of the issues involved with making progress that will improve care. In particular, as CMS discusses in the rule, the percentage of PAC use and multiple transitions reinforce the need for improvements around transitions of care. According to ONC in their "Health IT in Long-term and Post Acute Care Issue Brief" dated March 15, 2013, "In 2008, almost 40 percent (38.7%) of all Medicare beneficiaries discharged from acute-care hospitals received post-acute care."

CHIME agrees with CMS' assessment of the drivers for the persistent challenges for improving care transitions and the care continuum overall. CHIME members have firsthand experience demonstrating that poor patient outcomes, resulting from poor communication and lack of information about patients, can contribute to hospital readmissions, emergency department (ED) visits, and adverse outcomes. CMS also notes that many long-term and PAC, behavioral health, and home and community-based service providers have not adopted health IT at the same rate as acute care hospitals in large part because these providers were not eligible for the Medicare and Medicaid EHR Incentive Programs. This difference slowed the adoption of EHRs and other forms of interoperable health IT for these providers.

In their 2017 report, the American Hospital Association stated that an average-sized hospital dedicates 59 full-time equivalents (FTEs) to regulatory compliance, more than one-fourth of which are doctors and nurses. While an average-size community hospital dedicates 59 FTEs overall, post-acute care regulations require an additional 8.1 FTEs.[10] Thus, more relief from administrative burden for PAC providers is needed. Further, in looking at how we can foster better communication and interoperability across the care continuum, especially between acute care and PAC, we encourage the Agency to develop incentives – rather than a "stick" approach – to facilitate adoption of interoperable health IT systems and use of these interoperable data across settings, including long-term and PAC. Regarding PAC providers, CMS could consider financial support for technology adoption such as:

- Payment of any initial or setup fees for a PAC Provider to join an HIE or HIN;
- Increasing reimbursement by 2% for providers that send and receive data electronically;
- Reimbursement to PAC providers for costs of apps to meet interoperability during transitions of care;
- Funding to facilitate participation by PAC providers in a more collective "eConnected Alliance" for prescriptions drugs; and
- Promote the use and access to the connected e-prescription network to patients and families to look up their own drug history to be aware of their prescribed drugs and precautions they need to know to continue their recovery at home.

Additionally, CMS working with ONC could create an 'interoperability test' (i.e. for APIs), similar to the C-CDA Validator or scorecard by HealthIT.gov and found at https://sitenv.org/sandbox-ccda/ccda-validator. This kind of scorecard could assess the security and functionality (interoperability with a set of standards) of an app. This kind of scorecard could then be used as a "requirement" in future rules. This would also eliminate any delay in the current process for an EHR becoming certified, especially when it relates to one specific component (interoperability) which would be tested. While we recognize it would be costly to create and maintain, it could be helpful for future interoperability functionality as everyone would be building to the same standard and would be able to test to that standard.

CHIME also supports CMS' work to develop agreed-upon measure concepts that could inform analysis of how well providers are routinely and effectively engaging in exchange of information across settings. As CMS stated, to date, the measurement of interoperability has largely focused on the use of certified technology and the percentage of information exchanged. Expanding the scope of interoperability measurement beyond settings that were eligible for the EHR Incentive Programs is critical as efforts are being made to enable health IT and exchange capabilities

[10] American Hospital Association, 2017 Assessing the Regulatory Burden on Health Systems, Hospitals, and Post–acute Care Providers, https://www.aha.org/guidesreports/2017-11-03-regulatory-overload-report

across a broader range of care settings. It's worth noting that sometimes a vendor has capabilities, but the provider has not turned them on because they either aren't aware of it or don't know how to turn it on.

CMS also contemplates whether hospitals and physicians should adopt the capability to collect and electronically exchange a subset of the same PAC standardized patient assessment data elements (for example, functional status, pressure ulcers/ injuries) in their EHRs. The agency believes that since these health care providers have generally been eligible for the EHR Incentive Programs, many of them would have adopted certified EHR technology and health IT systems, which are required to capture and exchange certain data elements under the ONC Health IT certification program. With ONC's proposal to adopt USCDI Version 1, the set of data which systems must include under the certification program is set to expand in the coming years and would establish a minimum set of data classes that would be required to be interoperable nationwide. As CMS contemplates these and others ~~s~~ issues, we have outlined below several topics, which if addressed, could foster better information sharing between acute settings and PAC and other settings of care ~~not~~ ineligible for the HITECH monies:

- **Timely access to patient information:** First, most providers serving the PAC setting need the data before the patient is transferred. For example, for the PAC setting of inpatient rehabilitation, a preadmission screening is required by CMS. The preadmission screening is a detailed and comprehensive evaluation of the patient's condition and needs for rehabilitation therapy and medical treatment that must be conducted by a licensed or certified clinician(s) within the 48 hours immediately preceding the IRF admission. This screening is the initial determination of whether the patient meets the requirements for IRF admission. Additionally, while a physician extender can complete the preadmission screening, the rehabilitation physician concur that the patient meets the requirements for IRF admission. A rehabilitation physician must review, sign, and date the screening before the patient is admitted to the IRF.

  The content of a typical prescreen is information that is usually manually transcribed from an EHR and accompanied by "printouts" of EHR patient information. Another example is the use of discharge planning portals which acute care hospitals use to alert potential receiving providers that they have a patient and need a location to send them (i.e., needs rehab bed). While these portals are valuable, they typically do not provide enough information to make the best patient-focused transition of care decision. Because of CMS requirements, facility capability, and the specialty needs of patients, etc., receiving providers like rehabilitation facilities need specific information (i.e., medication lists) on the patient to determine whether they can accommodate them. Having this data in advance is helpful, but today there is no widely adopted electronic process for sharing this information. It should also be noted that there can be HIPAA interpretation challenges when the receiving provider does not yet have a relationship with the patient but needs information in order to assess whether they can accept the patient or not.

  Second, once it is decided where a patient will be transferred, access to timely information on the patient is critical. Unfortunately, receiving CCDs in a timely manner from acute care providers continues to present challenges regardless of whether the PAC provider uses an HIE or whether they are receiving Direct Messages. Some post-acute providers are often receiving information 3-4 days after transfer when they need the information in advance of the transfer, to ensure optimum care for the patient. Typically, the transition of care process is a vulnerable time for a patient and especially older adults and those with multiple comorbidities which are compounded by the lack of actionable patient data. This can result in an incomplete picture of the patient, which is typified by duplicative diagnostic tests (lab, radiology, etc.),

medication reconciliation challenges, patient dissatisfaction, and patient safety issues. This can lead to delays in transfer and therefore delays in recovery, as the patient waits until appropriate information is gathered and medical conditions are fully understood within the proper context of the individual's need.

There appear to be a few reasons why data is either delayed, not sent, or not acted on. While much of the needed data is being sent by EHRs via fax or HIE, it does not always arrive in time for the receiving provider to act upon the information at admission. Part of this challenge is rooted in a concern that providers and their EHR vendor may not be sending "all the information" or that the information may be incomplete. Another issue we hear is that clinicians do not trust the source of the data, whether that data comes from the post-acute, long-term care, acute or ambulatory settings. Data standards shared in a timely way can address data integrity and interpretation issues, as well as foster more meaningful use and trust in the data. It is important to note that when the context is shared along with the exchange of information, it will result in a shared understanding and better outcomes for the patient.

In CMS' FY 2019 final rule for skilled nursing facilities, the agency requires these providers to obtain certain information from acute hospitals, for example, to record the type of inpatient surgical procedure performed during the prior inpatient stay. Information flowing in both directions (between acute and post-acute / long-term care) is especially critical to foster better patient care. There is as much need for the acute-care setting to get information from the post-acute / long-term care settings when a patient is transferred as there is when a patient is being discharged from a hospital. We believe there is an opportunity for the post-acute / long-term care community, the acute care community, and CMS to work collaboratively to help patients avoid costly readmissions. One of the biggest ways we think this can be successful is with a greater emphasis on medication reconciliation. We do not, however, believe that a regulatory mandate or "stick" is the right approach to tackling these issues. Unless the issues around timely receipt of information are addressed, barriers will continue to exist, and technology alone will not address these underlying issues.

Strengths to build on:

a. **Medications & Data Element Library:** We continue to support the work CMS has undertaken surrounding the Data Element Library (DEL). While the DEL contains medications, the full list is not there. We recognize that CMS is working to build this out and that CMS is seeking further input on these topics under the "Transfer of Health Information & Care Preferences When an Individual Transitions – Medication Profile Draft Measure." We want to ensure that this work is aligned with what CMS is proposing under the USCDI.

   CMS is developing – with stakeholder feedback – a cross-setting, post-acute care transfer of health information (TOH) and care preferences quality measures in alignment with the Improving Medicare Post-Acute Care Transformation Act of 2014 (the IMPACT Act). The medication profile is part of the draft measure on TOH, which is the last of the domains that the IMPACT Act requires for LTCHs, IRFs, SNFs, and HHAs. It is our understanding that because it's an IMPACT Act measure, that the feedback received by CMS on this measure will be incorporated into the DEL. Since CMS believes that certain USCDI data elements would need to be exchanged in order to appropriately respond to the TOH measure on a patient assessment, it seems reasonable that there must be some glide-path to

incorporating the DEL into the USCDI to foster better interoperability between acute providers and PAC providers. In addition, there is value to "encouraging" acute settings to utilize this same data set when discharging a patient and sharing this information prior to or at the time of discharge.

- **Pediatrics:** In pediatric rehabilitation, there are several public agencies involved in the care, and they need to be included in data sharing.

- **Telehealth:** More reimbursement for PAC providers to support telehealth could also support the care continuum. One member who is expanding telehealth reported their organization spent $600,000 last year to send patients back for routine follow-up appointments with acute care clinicians, such as post-surgical visits. As a PAC provider, they are absorbing these costs and examining ways to offset it. Our member also reports hiring more physicians, such as internal medicine specialists, to handle medical needs during their inpatient rehabilitation stays. However, these changes carry additional costs, and as such they are exploring ways to help offset the costs, such as augmenting care with telehealth services that are reimbursed by Medicare.

- **Prior authorization and Da Vinci:** Facilitating prior authorization through the EHR could be helpful. For instance, if an acute provider could send an API call out to the payer on prior authorization this might mitigate some burdens faced by PAC providers. Extending this further, the call out from the acute providers looking for a PAC setting of care to transfer patients could be done leveraging technology to locate a receiving PAC specialist or bed available and the prior authorization could occur concurrently.

- **Pilots:** More integration between acute EHR vendors and post-acute vendors is needed. For instance, CMS could consider a pilot to develop the ability of PAC vendors to better consume data from the acute setting to improve care handoffs, efficiency, and outcomes. Having a model for other PAC providers to use would provide value.

  Some work has already been done at the state level and this could be used as a starting point for examining pilots at the federal level. For instance, Georgia has an effort around fostering information sharing across the care continuum.[11]

  Another option could be exploring further use of Direct. While we recognize that Direct does not result in semantic interoperability by delivering a PDF, it is better than no data being shared. We are aware that small PAC providers are particularly lagging with technology adoption and are resource-strapped. Support for smaller providers, thus, could be particularly helpful in speeding data sharing among these providers. One of our PAC members was required to participate in an HIE, and, while the standard was not Direct, it was a standard data file. Fostering information sharing, again, is possible, but PAC providers need help, especially since they were not authorized to receive HITECH monies.

[11] https://dph.georgia.gov/sites/dph.georgia.gov/files/related_files/site_page/Concentration%202%20Communication%20Combined.pdf and http://www.pathway-interact.com/wp-content/uploads/2017/04/148604-Hospital_to_Post_Acute_Care_Transfer_Form.pdf

- **Alignment of incentives:** Incentives for sharing data should be properly aligned to support sending and receiving parties. Part of the challenges in achieving better information exchange between acute and PAC providers will be rooted in vendors (some of whom are not certified) working together to foster better interoperability.

- **Testbeds:** ONC has a testing tool which can be used to help providers and vendors improve their CCD's interoperability. However, the standards must be "tightened" to reduce variability. For instance, one member reported that when using the tool to test moving data from vendor A to vendor B he found that for problem lists vendor A placed the English label for entries in the problem list only in the human-readable section of the CCD, but vendor B required the English label in the machine-readable section. While both versions could pass the ONC testing tool, the result was vendor B displayed the problem list showing only the LOINC codes rather than a label understandable to providers. As a result, this member was forced to come up with LOINC codes and had to manipulate the file before ingesting it so that the English version showed up in the correct place.

  In addition to needing tighter standards, we believe providers and vendors would benefit from pilots or other standardized testing mechanisms that allowed them to test the functionality for transmitting discharge information to a PAC provider from an acute provider .Prior to this, identifying and agreeing upon the data elements most needed by each setting of care must occur.

Recommendations to consider: ONC and CMS should:

- **Enhance the policy and operational support to focus on improving the ability of receiving providers to ingest actionable data;**
- **Engage stakeholders to develop more innovative incentives (financial or otherwise) which encourage better information sharing between acute settings of care and PAC, such that it results in effective "moments of sharing";**
- **In fostering information sharing, a "carrot" rather than a "stick" approach is needed;**
- **Remove regulatory and administrative burdens for PAC providers;**
- **Support greater use of telehealth in PAC settings to reduce costs;**
- **Encourage and support providers to leverage technology to speed the location of beds/facilities for patients being moved from an acute care setting to a PAC setting, including the use of prior authorization via the EHR to help speed the process;**
- **Create a pilot or test environment to demonstrate the extent of interoperability for information received by a PAC from an acute care provider. This testing requires advance work to identify and agree upon the data elements most needed by each setting of care;**
- **Ensure the "Transfer of Health Information & Care Preferences When an Individual Transitions – Medication Profile Draft Measure," is aligned with what CMS is proposing under the USCDI; and**
- **Create a glide-path to incorporating the DEL into the USCDI to foster better interoperability between acute providers and PAC providers.**

X. Revised and New 2015 Edition Criteria

ONC recognizes that health care providers need health IT that stores data in structured formats. In support of these objectives, ONC proposes to adopt revised and new 2015 Edition certification criteria, including new standards. The proposed updates include the following:

2. USCDI
3. Electronic Prescribing Standard and Certification Criterion
4. Clinical Quality Measures
5. Electronic Health Information Export
6. Standardized APIs for Patient and Population Services Criterion
7. Privacy and Security Transparency Attestations
8. Data Segmentation for Privacy and Consent Management

Given the magnitude of the changes ONC proposes, we believe a better and more reasonable approach to updating the 2015 Edition **would be to create a new edition**. Our recommendation is consistent with the HITAC's Conditions and Maintenance of Certification Requirements Task Force, which found, "There are broad-sweeping changes to the 2015 Edition as a result of this proposed rule. By not updating to a new Edition, users of the CHPL would be confused about which version of 2015 Edition is being referenced."

Additionally, we believe ONC has not allowed adequate time to implement the extensive changes it proposes, whether these are advanced as updates to the 2015 edition or, as CHIME recommends, as a new edition. The proposed 24-month timeline does not take into account the time providers need to get into the queue to receive the new software, train on the new system, or adapt workflows -- the latter two pieces which have historically been critically necessary. Furthermore, rushing deployments and installations can present threats to patient safety.

Below, we offer comments on specific elements of ONC's proposal to update the 2015 Edition with revised and new requirements including USCDI, EHI export, APIs, privacy and security, and data segmentation.

Recommendations: We recommend ONC:

1. **Not proceed with their plans to update the 2015 CEHRT to accommodate a staggering array of changes, and instead, plan for an entirely new edition; and**
2. **Adopt a longer timeframe for vendors and providers to absorb these changes. At a minimum we recommend 36 months.**

USCDI

ONC discusses the ongoing transition toward value-based care and the inclusion of data classes that go beyond clinical data. ONC says that to advance interoperability by ensuring compliance with new data and vocabulary codes sets that support the data, they have proposed removing the "Common Clinical Data Set" definition from the 2015 Edition and replacing it with the "United States Core Data for Interoperability" (USCDI) v1 standard. In doing so, ONC refers to the USCDI as "a standardized set of health data classes and constituent data elements that would be required to support nationwide electronic health information exchange." Developers would be required to update their certified health IT to support the USCDI v1 for all certification criteria affected by this proposed change. And, unless prohibited by the Secretary, health IT could continue to be certified or upgraded to a newer version of

an identified minimum standard code set than that included in USCDI v1 or the most recent USCDI version that the National Coordinator has approved for use in the Program through a new process they are calling the Standards Version Advancement Process.

CHIME supports replacing the Common Clinical Data Set with the USCDI v1. We have long advocated for the need for greater uniformity in the use of standards and support HHS taking this step. The USCDI v1 contains updates from the initial version published in January 2018. New data elements include: address and phone number; pediatric vital signs; clinical notes; provenance (author, time stamp, and author's organization); and unique device identifier(s) for a patient's implantable device(s).

Recommendation:

CHIME supports replacing the CCD with the USCDI and making it a standard. We also support ONC following a predictable, transparent, and collaborative process to expand the USCDI.

Electronic Health Information Export

ONC proposes to replace the data export criterion within 2015 CEHRT, which uses the CCDA standard with a standards agnostic approach using a new 2015 Edition revised base certification criterion for EHI export. ONC says their approach is intended to provide patients and health IT users with a means to efficiently export the entire EHR for a single patient or all patients in a computable, electronic format. ONC says that they ultimately anticipate all data to be transferred through APIs or other advanced technologies. We appreciate that ONC is pushing toward API-based exchange, and ideally it would be more effective to mandate a standard like FHIR as they did for the patient exchange. However, we understand that the intention is likely that ONC didn't want to immediately halt all conversion capabilities that currently exist. Writing to the EHR will be the final hurdle. All the major EHR vendors are already offering a query/read capability on these resources, however the write functionality supports significantly fewer resources today.

ONC also states this approach better supports interoperability and importantly notes that the new EHI export criterion differs significantly from the "data export" certification criterion as the new approach is not limited to clinical data as specified in the CCDA. Rather, it applies to all produced and electronically managed EHI. The agency further proposes that developer rollout of the "EHI export" would be required within 24 months of the effective date of the final rule. ONC sought feedback on whether the request for an EHI export should be limited to ONC proposed criterion for export functionality to support two specific use cases:

1) Patient access to data: a patient's access to their EHI and a provider's ability to switch to another health IT system. Regarding the patient-focused export capability, the health IT certified to this criterion would have to enable the export of EHI for a single patient upon a valid request from that patient or a *user* on the patient's behalf. ONC believes this capability complements other provisions of the proposed rule that support patients' access to their EHI, including information that may eventually be accessible via the APIs. ONC states that it expects all data to be transferred through APIs or other advanced technologies.

2) Providers switching vendors: This criterion would support the export of EHI when a healthcare provider chooses to transition or migrate information to another health IT system. By providing at least a baseline capability for exporting EHI in a commercially reasonable format, ONC believes that this criterion would

help to address some of the potential information blocking practices and enable smoother transitions between health IT systems.

CHIME members appreciate the need to support the two use cases described above. We worry, however, that the ONC proposal involves exporting data that is contained in both certified and non-certified products as the proposal applies to all data produced and electronically managed under the EHI definition. We question, for instance, how a provider could be expected to export data from a non-certified product that may not be readily exportable. The burden for ensuring this data can be exported will fall to providers, since, under the rule as currently proposed, these other vendors are not governed by ONC. Also, as discussed earlier, ONC's definition of developer presently only includes those vendors with at least one product on the CHPL, therefore, it remains unclear how a provider could compel a vendor who is not certified and has no certified products to help export data. Therefore, as noted earlier, we believe the data should be limited to what is contained in the legal medical record. We agree with the HITAC's Conditions and Maintenance of Certification Taskforce which called for limiting the EHI export scope/certification criteria to what is in the legal medical record and retained in the certified HER. .[12]

Finally, ONC also says in the rule that typically a provider or his or her office staff will be performing the request for an EHI data export on behalf of the patient, given that a request of this nature would likely occur in the context of an individual exercising the right of access under the HIPAA Privacy Rule. ONC says a developer could develop a method that allows the patient using a technology application (e.g., portal or "app") to execute the request without needing a provider to do so on their behalf. ONC requested comment on whether this portion of the criterion should be made more prescriptive to only allow the patient and his or her authorized representative to be the requestor of their EHI, similar to how they have previously scoped such criteria as "view, download, and transmit to 3rd party." CHIME believes that it should be limited to the patient or their authorized representative.

Recommendations:

1. **The scope of EHI is too expansive and should be limited to what is contained in a certified product that is part of the legal medical record; and**
2. **ONC should only allow patients or their authorized representative to be the requestor of their EHI.**

Standardized APIs for Patient and Population Services Criterion

ONC proposes to adopt a new API criterion that would replace the "application access – data category request" certification criterion and become part of the 2015 Edition Base EHR definition. This new certification criterion would require the use of FHIR standards, several implementation specifications, and focus on supporting two types of API-enabled services: 1) services for which a single patient's data is the focus; and 2) services for which multiple patients' data are the focus.

We have detailed our comments on APIs under the section titled, "Conditions and Maintenance of Certification."

Privacy and Security Transparency Attestations

ONC has proposed to add two new 2015 Edition privacy and security "transparency attestation" certification criteria for: 1) encrypt authentication credentials; and 2) multi-factor authentication. ONC is calling for vendors to attest

[12] https://www.healthit.gov/sites/default/files/facas/2019-04-25_CMC_TF_Presentation.pdf

that they either do or do not have this capability. Vendors, however, would not be required to have this functionality even though it is currently inexpensive and ubiquitous. CHIME is not aware of any reasonable justification for making encryption an optional part of certification, and other expert entities have called for such a requirement.

Late last year the public-private Joint Cybersecurity Workgroup published, "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients,"[13] (HCIP), which recommends the need to encrypt among its recommendations. In fact, this Workgroup clearly cited the lack of encryption as a vulnerability.

And, as referenced earlier, the Health Care Industry's Cybersecurity Task Force[14] report issued in June 2017 devoted much attention to cybersecurity issues with EHRs. The report makes several recommendations to improve EHR security, including requiring strong authentication to improve identity and access management for healthcare workers, patients, and medical devices / EHRs. The report recommends that, "In situations where the provider is accessing an EHR or Health Information Exchange external to the hospital or clinical environment, the health care industry should adopt the NIST SP 800-46 guidelines for remote access including the use of two-factor authentication to ensure a compromised password cannot alone be used to gain access." Finally, having the capability to do single sign-on would remove several administrative burdens for clinicians and should also be offered.

Recommendations: ONC should require:

1. **Vendors to offer encryption and multi-factor authentication, as well as single sign-on capabilities, to all their clients under their certification requirements, rather than just having to attest that they do or do not offer these features. This will help offer further tools to providers fortify their systems and ultimately will protect patients; and**
2. **Prohibit vendors from using default passwords, another known vulnerability in healthcare.**

XI. Conditions and Maintenance of Certification

The Cures Act requires that health IT developers comply with certain Conditions and Maintenance of Certification concerning:

1. Information blocking;
2. Assurances around the appropriate exchange, access, and use of electronic health information;
3. Communications regarding health IT;
4. Application programming interfaces (APIs);
5. Real world testing for interoperability;
6. Attestations regarding certain Conditions and Maintenance of Certification requirements; and
7. Submission of reporting criteria under the EHR reporting program.

CHIME has the following feedback to offer on select requirements under the MOC. As a preliminary matter, as recommended above under our patient matching comments, we believe that to better foster interoperability as part of their MOC requirements vendors should be required to share their patient matching rate with providers.

[13] https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf
[14] https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf

Recommendation:

ONC should require vendors to share their patient matching rate with providers as part of their MOC requirements.

Assurances

The Cures Act requires that a health IT developer, as a Condition and Maintenance of Certification, provide assurances that it will not take any action that constitutes information blocking, or any other action that may inhibit the appropriate exchange, access, and use of EHI. To implement this broadly worded requirement, ONC proposes more specificity for the required assurances. CHIME supports the additional detail ONC proposes.

Our members reported situations where they bought a system that the vendor said meets the requirements. However, upon implementation, providers learned that the product does not work as promised or advertised. CHIME appreciates ONC's work to improve transparency around the purchasing process and particularly ONC's focus on ensuring products are more interoperable.

In reviewing this proposal, we identified one concern. ONC has proposed that a developer must, for a period of ten years beginning from the date of certification, retain all records and information necessary that demonstrate initial and ongoing compliance with the requirements of the ONC Health IT Certification Program. However, they state that if the applicable certification criteria are removed from the Certified Health IT Product List (CHPL) before the ten years have expired, records must only be kept for three years from the date of removal unless that timeframe would exceed the overall ten year retention period. Given some of the situations associated with vendors being sanctioned for passing certification and not having the promised capabilities, and the liabilities this exposes providers to (i.e. federal audits and malpractice), we believe records should be maintained indefinitely. For instance, under the Promoting Interoperability program, audits can reach back as far as six years under some policies[15] and ten for others.[16]

In addition to records retention policies, under Assurances ONC also discusses the Trusted Exchange Framework (TEFCA). The Cures Act requires ONC create a voluntary TEF and Common Agreement for the purpose of ensuring full network-to-network exchange of health information. ONC requested comment on whether health IT developers should be required to participate in the 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. After publication of this information blocking rule, ONC subsequently published Draft 2 of TEFCA. CHIME is reviewing the second draft and looks forward to offering our feedback through that comment process.

[15] https://www.cms.gov/regulations-and-guidance/legislation/ehrincentiveprograms/downloads/ehr_supportingdocumentation_audits.pdf
[16] https://www.federalregister.gov/d/2010-17207/p-1722

Recommendations:

ONC should retain records of products on the CHPL indefinitely. Providers need this information to defend audits and lawsuits. At a minimum, it should be no less than the time CMS and other federal entities can recoup monies, such as under the Promoting Interoperability program.

Communications

The Cures Act placed no limitations on the protection of the communications (i.e. gag clauses) between vendors and providers, and ONC has proposed to broadly interpret the subject matter of communications that are protected from violations of their Maintenance of Certification. ONC says, "any prohibition or restriction not expressly permitted would violate the Condition," of their certification. Further, the burden will be on the vendor to demonstrate they have met all of ONC's requirements. ONC points out, however, that a customer's dissatisfaction with a product is not necessarily indicative of the vendor engaging in restricted or prohibited communications. There are six classes of communications ONC identified where vendors would be prohibited from restricting communications:

- Usability of Health Information Technology;
- Interoperability of Health Information Technology;
- Security of Health IT;
- User Experiences;
- Manner in which a User has Used Health IT; and
- Business Practices Related to Exchange.

ONC does, however, recognize that there are circumstances where it is both legitimate and reasonable for developers to limit the sharing of information about their products. As such, ONC proposes a two-part test that would allow developers to impose prohibitions or restrictions on protected communications in certain circumstances that would allow a vendor not to share information about their product when both conditions are met: 1) "Communications with unqualified protection" which translates to when communication are related to a category ONC has established as being protected areas where vendors may not restrict information then they automatically fail the two-part test; and 2) they communications must fall into a narrow category ONC is calling "Permitted prohibitions and restrictions" (i.e. vendors communications with their own employees and non-user facing aspects of the product).

CHIME applauds ONC for the thoughtful approach to this topic. Providers have long been plagued by gag clauses and some have repeatedly been prohibited through contracts to share information like screen shots, even if it was related to patient safety.

We have one concern, however, related to the amount of time ONC has proposed allowing for vendors and providers to change their contracts. ONC has proposed developers must notify all customers with whom it has contracts within six months of the effective date of the final rule regarding any contract / communication that must be amended pursuant to these new rules where it contravenes what is already in place. Then, annually thereafter vendors would be required to notify customers concerning the need to make changes to contracts. Vendors would have up to two years to remove any contravening provisions related to communications. We appreciate that ONC has recognized the urgency around the need to correct the persistent challenges providers face in this space. But,

we worry about both providers and vendors' capacity to execute all of the necessary changes in such an abbreviated timeline.

Finally, we were pleased to see ONC's discussion around cybersecurity and threat sharing. Although the Department for Homeland Security (DHS) together with the Department of Justice (DOJ) published voluntary guidance[17] around threat sharing in 2015 stemming from provisions contained in the Cybersecurity Sharing Act of 2015 (CISA). Despite the guidance that was published, providers continue to experience barriers around threat sharing activities, and frequently information is still not shared. Sometimes the reasons for this are rooted in prohibitions in their contracts with vendors.

ONC proposes that if developers were to impose prohibitions on communicating information about cybersecurity threats and incidents to government agencies, that this would not comply with this Condition of Certification. ONC seeks comment on whether it would be reasonable to permit health IT developers to impose limited restrictions on communications about security issues to safeguard the confidentiality, integrity, and security of eHI. ONC asks whether developers should be permitted to require users of health IT (providers) to notify the developer about the existence of a security vulnerability prior to, or simultaneously with, any communication about the issue to a government agency?

We support making it a violation of the maintenance of certification for a vendor to prohibit communications about cybersecurity threats. However, we fail to understand why providers would be required to notify the developer about the existence of a vulnerability. The threats that exist are ones that pose risks to providers and the patients they serve. We are unclear what problem is solved by imposing an additional requirement for providers to report vulnerabilities to vendors. Further, typically providers are not the controlling entity or best-positioned for sharing threat information. In fact, they are often prohibited by contract from doing so.

Recommendations: CHIME strongly supports ONC's proposal to remove restrictions vendors place around communications associated with their product, including matters pertaining to security. We offer three recommendations to strengthen this section of the proposed rule:

1. **Given the complexity associated with changing contracts and the volume of contracts providers have with vendors, we request that ONC provide more than the allotted 24 months for this to occur. We recommend instead that ONC allow up to five years.**
2. **ONC should make it a violation for vendors under information blocking requirements and their maintenance of certification to not share cyber vulnerabilities with providers; and**
3. **Pertaining to cybersecurity, providers still have significant reservations around sharing known vulnerabilities and threats given contracts and other barriers. ONC should work collaboratively with DHS to mitigate these sharing issues given the highly sensitive nature of health information and the threats faced by our industry. And, as outlined above earlier in our letter, we have significant security concerns around APIs.**

[17] https://www.govinfo.gov/content/pkg/FR-2016-06-15/pdf/2016-13742.pdf

APIs

Standards

The Cures Act requires that patients be able to access their information via APIs "without special effort." ONC proposes to adopt FHIR Release 2 as the baseline standard for a new API standard, citing that itis widely adopted. While they explain that FHIR Release 3 is published and some health IT developers have included varied support for it in their product(s) at this time, ONC reports there is limited evidence that its production deployment is as widespread as FHIR Release 2. Instead, ONC expects FHIR Release 2 would provide a stable and consistent direction in which the industry can go when it comes to deploying (g)(10)-certified APIs that support data access to the USCDI. ONC also notes that FHIR Release 4 has now been published and seeks comment on how it should adapt to its proposals to reflect the evolving maturity of standards use. They furthermore list four options for public consideration around the FHIR standard adoption:

1. **Option 1:** Adopt just the FHIR Release 2 (proposed by ONC)
2. **Option 2:** Adopt FHIR Releases 2 and 3
3. **Option 3:** Adopt FHIR Releases 2 and 4
4. **Option 4:** Adopt just FHIR Release 4

ONC has only proposed 24 months to transition to Release 2. While we believe that moving to Release 4 is preferable, we are concerned about the readiness of the industry to accomplish this in the short, proposed timeline of 24 months from the time the final rule is published. There are providers and vendors at different levels and adequate time is needed for the industry to adapt. It is our belief that those who are already leading with the use of FHIR start with either Release 2 or 3. Further, at the Argonaut council meeting held in February it was largely agreed, including input from some of the vendors, that the industry should move forward with Release 4..

ONC furthermore states that its proposal to adopt the FHIR standard alone is insufficient to provide the level of consistent implementation that will be necessary to meet the Cures provision that calls for patient access to their data via APIs "without special effort." To address this challenge, ONC proposes an implementation specification that would list a set of base FHIR resources that Health IT Modules certified to the proposed criterion would need to support. ONC proposes an initial set of 15 FHIR resources – the "API Resource Collection in Health" or "the ARCH" – that would align with and be directed by the data policy specified in the proposed USCDI standard. The challenge today is that everyone is adopting their own profiles right now. If providers and vendors are implementing FHIR resources in different ways, we will still experience interoperability challenges, therefore, tighter integration is needed.

Recommendations: We recommend ONC:

1. **Select Release 4 as it is the most ideal scenario, and provide additional time for its adoption (variation of Option 4);**
2. **Provide at least three years from the time the final rule is published for vendors and providers to move to FHIR to achieve FHIR fluency under Release 4; and**
3. **If starting with Release 4 is not possible, then begin with Release 2 and then move to Release 4 (variation of Option 3).**

Security

CHIME received a tremendous amount of feedback from members regarding the security aspect of ONC's API proposal. Our concerns are rooted in security and privacy issues, including:

- **Validating scope of access:** We read ONC's to require that providers outsource their identity management. Currently, if providers have a trusted actor – someone they routinely do business with and know well – the provider has a comfort level with granting access to their system. In these situations, when a patient requests access to their data, the provider has a strong level of assurance that this is a good actor. However, it appears from the proposal that ONC is asking providers to trust other entities to do the identity management for third parties they do not know. It also appears ONC is assuming that the software developers are doing identity management and finding the right record. We agree that patients must be able to get data in a simple manner, but if a provider cannot validate software let alone validate that its secure, then we believe we will be exposing the healthcare system and patients to unnecessary risks.

  Validating the scope of access to patient data via a third-party app presents challenges. Granting access to third parties entails getting a token from an app developer to access the API. The access granted by a patient is based on a token from a developer, which should match the authorization that the patient gave. If the app developer tells the provider that the patient granted access, then the provider would then grant the access. However, under this proposal providers will lack the ability to routinely audit or validate the scope of authority that was granted by individuals to the third-party app developer represented in the token they receive. In any case where the data being requested is not a comprehensive record and access should be restricted to limited data elements, our members questioned how they would be able to ensure that the data being extracted is being limited to what was authorized by the patient. There is also no way to trace back to the patient that they have only granted access to a partial amount of their medical record. Therefore, providers are, in essence, taking the word of the developer to authorize access. For apps known to a provider this may be less of any issue. However, it presents challenges to providers when the app is unknown.

- **Nefarious actors and good cyber hygiene:** Our members also have significant concerns about "honey potters" and fly-by-night operations that increase fraud in our system and put patient data at risk. Under ONC's proposal, there is an assumption that anyone making a credible claim for access to a provider's system is doing so under the auspices of requesting access to patient data. Our members have reported instances of fake healthcare facilities requesting access to their systems – known as "honey potters" – entirely for the purposes of getting access to data they shouldn't have. To outside providers, these entities appear to be legitimate. Take the example of a patient who says they have an app to monitor their health, and requests the provider send their data. The provider would have no idea where the data is actually going without having a way to validate it, which they would not. We are very concerned that what sounds like the improbable could create significant opportunities for abuse. As one member stated, "It doesn't make it easier; it makes inevitable." Our members have concluded that there must be some system of meaningful authorization, yet they are not sure there will be any system that is better than the one today.

- **Validating apps:** A significant issue identified by our members is that under the Administration's proposals providers will have no way to ensure that vendors have gone through a systematic process to validate an app from a security standpoint. While some big vendors appear to be doing a good job of interfacing with the large technology companies in the app management ecosystem space, this is not yet a widespread practice nor is it mandatory. Our members are concerned that some apps / third parties may take patient data and use it in ways not known to patients, as we have seen with some large technology companies. Therefore, they firmly believe that more must be done by the government to help ensure this does not happen. We fully agree patients have a right to their data; nonetheless, the news coming out daily around inappropriate use of consumer data offers ample evidence that patients are very much at risk of having their health data used in ways they never intended or authorized.

- **Assumptions:** ONC appears to make the assumption that the authorization to access patient data is being managed appropriately and accountability and security is built in to manage this process, however as the rule is written these pieces are unclear. For instance, it's unclear to us how each provider is expected to know with any level of certainty whether vendors are meeting basic security principles and whether will be indemnified if they are not. It's worth pointing out again that the Health Care Industry's Cybersecurity Task Force devoted an entire section of their report to discussing challenges with EHRs, noting an insufficient amount of attention is being paid, especially in light of the increasingly interconnected healthcare system.

  Ultimately, CHIME believes that the proposed rules should seek to ensure the following: 1) is the entity seeking access authorized to obtain the data they are requesting and are they authorized to access the data via the API; and 2) the provider knows the entity before that entity accesses the data. The rule as written does not provide clear policies for addressing these issues. We seek clarification on ONC's expectations to ensure our interpretation is accurate. In addition, we wish to reiterate here our concern that this proposal does not align well with HIPAA. Our members are very familiar with HIPAA business associate agreements when sharing patient data and that has become the gold standard in the industry. Unravelling this standard could have significant consequences in light of the issues we have raised. Again, we must take reasonable and appropriate security precautions to safeguard data when it is requested by patients.

- **Business Associate Agreements:** Our members have reported some promising signs , with their engagement with mobile app management companies and app developers. However, this is far from widespread. Some members say that they are being asked for a Business Associate Agreement (BAA) by one large app development ecosystem management company. This is welcomed by our members since it gives the providers some level of control, for example to reject developers who may not meet the provider's security standards. As one member noted, "If we don't have a contract with them, we don't know what is implied." Another member noted that if their large vendor does not permit API access to an app then they will not grant any access. However, absent from having a contract, a safe harbor for providers will be needed to ensure that if data is shared inappropriately, the provider is protected. We spoke with this same large vendor who reported that they have a sandbox that it is completely open, and they have a white list and a gallery. The vendor reported that they ask clients to get involved, but once on the white list, any client can use it so that it's not an additional validation. Currently, our members are unsure if a BAA can be safely relied upon in this instance. They are also uncertain if an app developer's refusal to sign a BAA constitutes information blocking.

- **Certification of apps:** In discussing ONC's proposal we concluded that there needs to be an "arbiter of apps" – in other words, an entity that certifies them. We do not believe providers should be required to bear

all the risk for verifying apps under any circumstance. Nor should this fall exclusively to the vendors. Additionally, one only needs to look at some of the EHR vendors that passed ONC's certification process and were approved despite significant flaws and downstream implications for providers. It is hard for our members to fathom an environment where no one is authorized to provide some sort of "good housekeeping seal of approval" or certification process to apps. We believe this could be a role for a non-federal entity. As we envision it, apps that clear this certification process would be deemed eligible to connect with providers via an API. If an app didn't pass or seek certification, then a provider would not be required to connect. This would provide more assurance to providers and patients that the app was operating in good faith and adhering to a standard set of principles.

Recommendations:

1. **App management companies should be required to obtain a BAA with providers;**
2. **In the absence of a BAA, HHS should:**
    a. **Either offer a safe harbor to providers in the event that they offer access to a third-party app and this third party uses data in a manner that was not intended by the patient; OR**
    b. **Offer a safe harbor for providers who use an authorized / standard template agreement**

Real World Testing

The Cures Act requires, as a Condition and Maintenance of Certification, that developers have successfully tested the real-world use of the technology for interoperability in the type of setting in which such technology would be marketed. The objective of real-world testing is to verify the extent to which certified health IT deployed in operational production settings is demonstrating continued compliance to certification criteria and functioning with the intended use cases as part of the overall maintenance of a health IT's certification. Real-world testing should ensure certified health IT can share electronic health information with other systems.

ONC proposes to limit the applicability of this Condition of Certification to developers with Health IT Modules certified to one or more 2015 Edition certification criteria focused on interoperability and data exchange, which are the:

1. Care coordination criteria;
2. Clinical quality measures (CQMs) criteria;
3. "View, download, and transmit to 3rd party";
4. Public health criteria;
5. API criteria; and
6. Transport methods and other protocols criteria.

CHIME strongly supports real-world testing. As we discuss in our comments on the Care Continuum section of our letter, however, we are concerned that there has been too much focus on the export capabilities of systems and not enough attention paid to providers being able to ingest data. We believe more attention is needed to ensure there is greater semantic interoperability so that data is presented to clinicians in a more meaningful and facile way. Further, many "data blocking" issues stem from the inability of the receiving party to accept the data. One way to help accomplish this would be to require vendors to be able to accept and ingest their own CCD.

Additionally, we have questions about ONC's proposal, which notes that for the purposes of meeting the requirements for real world testing, "developers must provide the updated certified health IT to all their customers with health IT previously certified to the identified criteria no later than 24 months after the effective date of a final rule for this proposed rule. For the purposes of meeting this compliance timeline, we expect health IT developers to update their certified health IT without new mandatory testing and notify their ONC-ACB on the date at which they have reached compliance. Developers would also need to factor these updates into their *next* (emphasis added) real world testing plan." We question how this would work and worry that this would result in a scenario whereby vendors could deliver updated certified products without real world testing. Vendors who have already been deemed as re-certified may then choose not to engage in the real- world testing. This problem may be addressed if ONC decides to create an entirely new Edition rather than requiring changes to the existing 2015 CEHRT.

Finally, we agree with the HITAC's Conditions and Maintenance of Certification Requirements Task Force conclusion that it's unclear from ONC's proposal what will occur from a testing standpoint when there are no testing tools yet available for a new standard.

Recommendations: We recommend ONC:

1. **Focus more on the ability of receiving providers to ingest data;**
2. **Require vendors under real-world testing requirements to be able accept and ingest their own CCD;**
3. **Provide clarification around real world testing following an update to the 2015 CEHRT;**
4. **Provide a new edition of the current 2015 CEHRT that includes real-world testing; and**
5. **Offer clarification around how real world testing will occur when testing tools are not yet available.**

Data Segmentation for Privacy and Consent Management

ONC is proposing to remove the current 2015 Edition DS4P-send and DS4P-receive certification criteria and propose to replace them with three new 2015 Edition DS4P certification criteria (two for CCDA and one for FHIR). They state their approach would support a more granular approach to privacy tagging data for health information exchange supported by either the C-CDA- or FHIR-based exchange standards. We believe this proposal will support care coordination, navigating different state privacy laws and offer a more usable display of opioid use disorder (OUD) information.

While using the data tagging capability is much easier and a more elegant solution and FHIR permits you to add tags to data at a resource level, providers still must wrestle with varying state policies that create numerous complexities for managing this data. These challenges are not easily solved.

Recommendation:

It is also our understanding that tagging will be a feature of FHIR Release 4, but ONC's proposal is to move to Release 2 so we are unclear how this would work. It is also our understanding that neither Release 2 nor DS4P are backwards compatible and don't have as many resources as Release 4.

Conclusion

Together, these rules will have transformative effects on our members and the patients they serve. We thank you for the consideration and look forward to offering our feedback on these policy proposals. Please contact Mari Savickis, vice president, federal affairs, at mari.savickis@chimecentral.org with any questions you may have.

Sincerely,

Russell Branzell, FCHIME, CHCIO
CEO & President, CHIME

Clint Perkinson
Director, Information Technology
Vice Chair, AEHIT