America's Health Insurance Plans
601 Pennsylvania Avenue, NW
South Building, Suite Five Hundred
Washington, DC 20004

Matthew Eyles
President and CEO

June 3, 2019

Donald Rucker, M.D.
Department of Health and Human Services
Office of the National Coordinator for Health Information Technology
Attention: 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Proposed Rule
Mary E. Switzer Building
Mail Stop: 7033A
330 C Street, S.W.
Washington, D.C. 20201

Submitted electronically via www.regulations.gov

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

Dear Dr. Rucker:

On behalf of America's Health Insurance Plans (AHIP), thank you for the opportunity to offer comments in response to the Office for the National Coordinator of Health Information Technology (ONC) proposed rule on Interoperability, Information Blocking, and the ONC Health IT Certification Program published in the *Federal Register* on March 4, 2019 (RIN 0955–AA01).

AHIP is the national association whose members provide coverage for health care and related services to millions of Americans every day. Through these offerings, we improve and protect the health and financial security of consumers, families, businesses, communities and the nation. We are committed to market-based solutions and public-private partnerships that improve affordability, value, access, and well-being for consumers.

We applaud the Department of Health and Human Services' (Department's) continued efforts to promote transparency and accessibility of health information to support consumers in health care decision-making. Health insurance providers are committed to finding innovative ways to integrate and share data with consumers, doctors and hospitals. Improving access to meaningful information can help all Actors in the health care ecosystem to realize the full benefits of health information technology and data sharing—from improving care coordination to providing access to patient out-of-pocket cost and quality information—to achieving better health outcomes, more affordable care, and higher patient satisfaction.

Our comments and recommendations regarding the proposed rule reflect AHIP's commitment to continue our partnership with the Administration to develop policy solutions that will support a more consumer-focused market, ensure access to meaningful, actionable information, and promote quality and affordability. **AHIP and its members look forward to a public-private partnership across a multitude of stakeholders to make true interoperability of health information a reality.**
While we support the Department's efforts, AHIP and our member companies have serious concerns about the proposed rules which primarily focus in four main areas: the privacy and security of our beneficiaries' data, the use of data disclosed pursuant to these rules that could result in anti-competitive

behavior and the timing of the rules' implementation. Below we summarize our comments and recommendations on key issues. A more detailed compilation of our comments is included in the attached appendix:

Health plans need clear guidance on how ONC Certification requirements would apply to their application programming interfaces. AHIP supports the proposed new and revised 2015 Edition Certification Criteria (with the exception of the revised data segmentation for privacy (DS4P) criteria) as applied to certified health IT developers and providers using certified health IT products. While health plan-deployed application programming interfaces (APIs) required by CMS in the companion interoperability proposed rule do not need to be certified, CMS expects these APIs to meet standards comparable to the 2015 Edition Certification Criteria as if certified. However, neither CMS nor ONC have provided any guidance on which of the proposed new and updated Certification Criteria would apply to health plans, or how the Criteria should be implemented for those APIs. We recommend that CMS and ONC clarify in the final rule which of the new and revised 2015 Certification Criteria are applicable to health insurance providers deploying APIs.

ONC should clearly state that health plans are not included in the Information Blocking Provision. AHIP supports ONC's efforts to promote efficient exchange of information between health care stakeholders, and we support the intention of the information blocking provision. However, we believe that ONC's proposed definitions relating to the information blocking provision, specifically the definitions of Electronic Health Information (EHI) and Health Information Network (HIN), are too broad to be functional. ONC should leverage existing HIPAA definitions (e.g., the definition of electronic Protected Health Information [ePHI]) to help ensure clarity and consistency and build on the existing infrastructure and experience with HIPAA compliance. We recommend ONC clearly state that, in accordance with Congress' intent in the Cures Act, payers are not included in the definition of HINs and are thus excluded from the information blocking provision.

Inclusion of granular price information in the scope EHI could have unintended and anti-competitive consequences. ONC proposes to include "information that relates to the past, present, or future payment for the provision of health care to an individual" in the definition of EHI and seeks comment on the parameters and implications of including price information within the scope of EHI for purposes of information blocking. While we contend that information blocking does not apply to health insurance providers, the inclusion of such information in the U.S. Core Data for Interoperability would create comparable requirements under the CMS proposed rule. Shoehorning prospective price estimates in the definition of EHI in order to include it within information blocking is not substantiated by the underlying legal authority. HIPAA addresses availability of retrospectively provided service information to consumers and does not require prospective estimates be offered. The 21st Century Cures law provisions on interoperability focus on sharing information included in the clinical record. We do not believe ONC has the authority to mandate prospective pricing estimates as part of EHI.

AHIP and our members are firmly committed to providing consumers greater price transparency to aid in their decision-making and empowering them to choose health care services that are both affordable and right for them. Health plans offer transparency tools that give consumers estimates of anticipated costs and ways to compare services based on price, quality, and accessibility. Health plans recognize that existing tools require additional features and information from providers to allow for pre-service comparison shopping not currently available for some services. As an industry, we continue to innovate and lead the way in giving our members useable, practical, and understandable information to aid in their

decision-making. As ONC develops its final rule, we urge consideration of the unintended consequences of the release of granular pricing data on the progress private-sector health insurance providers have already made to provide tools and convey useful information to consumers.

Moreover, requiring public disclosure of pricing data could have potentially negative competitive effects that could hinder fair negotiations and drive up prices. According to the Federal Trade Commission (FTC), "…transparency is not universally good. When it goes too far, it can actually harm competition and consumers. Some types of information are not particularly useful to consumers, but are of great interest to competitors."[1] Should disclosure of private contract negotiations be required, the cost impacts could be significant, causing serious disruption to our health care system to the detriment of consumers.

ONC and CMS should harmonize efforts to identify reasonable circumstances that necessitate delay in or denial of requests for access to data. AHIP supports ONC's proposed exceptions to the information blocking provision, though we recommend ONC provide greater specificity as to the activities that would and would not be grounds for an exception. We recommend that ONC update the exception for promoting the security of EHI to indicate that, in addition to delaying access to data, an actor's attempts to thoroughly and sufficiently vet external locations of exchange (e.g., third party applications, networks) prior to sharing EHI should also not constitute information blocking. We also recommend CMS similarly identify and include in its companion interoperability final rule circumstances in which it may be appropriate for insurance providers to delay or deny a request by a consumer via a third-party app developer.

AHIP and its members are committed to working with the Administration and other stakeholders to advance greater interoperability and patient access to and control over their health information, with the ultimate goal of improving the quality and affordability of the care they receive. Along with our members, we thank you for allowing us to comment and look forward to a robust and collaborative process to bring this bold vision to reality. If you have any questions, please reach out to Danielle Lloyd, senior vice president for private market innovations and quality initiatives at either dlloyd@ahip.org or 202-778-3246.

Sincerely,

Matthew Eyles

Matthew Eyles
President and CEO

[1] Koslov, T. and Jex, E.; *Price transparency or TMI?;* Federal Trade Commission Blog; Jul 2, 2015 2:31PM; https://www.ftc.gov/news-events/blogs/competition-matters/2015/07/price-transparency-or-tmi.

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

AHIP Detailed Comments

SECTION IV – UPDATES TO THE 2015 EDITION CERTIFICATION CRITERIA

Revised and New 2015 Certification Criteria

ONC proposes to update the 2015 Edition by revising and adding new certification criteria that would establish the capabilities and related standards and implementation specifications for the certification of health IT. Specifically, ONC proposes to update the certification criteria by:

- Adopting the USCDI standard instead of the Common Clinical Data Set (CCDS),
- Updating its e-prescribing standard to match that of Medicare Part D,
- Creating a new "EHI export" criterion at the patient and provider level,
- Adopting a new "standardized API for patient and population services" criterion,
- Adopting an authentication encryption and multi-factor authentication criteria, and
- Adopting new "data segmentation for privacy (DS4P)" criteria at a more granular level (two for C-CDA and one for a FHIR-based API)

§ 170.213 United States Core Data for Interoperability (USCDI)

AHIP notes that while health plan-deployed application programming interfaces (APIs) required by CMS in the companion interoperability proposed rule do not need to be certified, CMS expects these APIs to meet standards comparable to the 2015 Edition criteria as if certified. As such, we are pleased to submit comments in response to the revised and new 2015 certification criteria with the understanding APIs should be expected to meet these standards. Under the proposed rules, we assume APIs would not need to meet Conditions or Maintenance of Certification requirements, as they are not subject to a formal certification process, therefore, we will not provide comments on those requirements. If ONC would like to explore this further, we welcome the opportunity to engage in additional conversations.

We also note that neither CMS nor ONC have provided any guidance on which of these criteria would apply to health plans, or how the criteria should be implemented for those APIs. **We recommend that CMS and ONC clarify in the final rule which of the new and revised 2015 Certification Criteria are applicable to health insurance providers deploying APIs.**

AHIP supports adopting the United States Core Data for Interoperability (USCDI) standard instead of the Common Clinical Data Set (CCDS) for the 2015 Edition Certification Criteria for providers and EHR vendors. We are supportive of the compliance timeline of 24 months after the effective date of the final rule if the relevant technical standards are available. We support ONC's intention to establish and follow a predictable, transparent, and collaborative process to expand the USCDI, including providing stakeholders with the opportunity to comment on the USCDI's expansion.

Clinical information is furnished to health insurance providers (sometimes in electronic format) for administrative purposes, quality reporting, risk adjustment and utilization management. While clinical

data is essential to get the payer-to-payer transaction to achieve the goal of providing continuity of care when someone changes issuers, this information is not generally helpful or useful at an individual patient level, through the payer-to-consumer transaction. For example, quality measures must be calculated across a population to be valid. In addition, both quality metrics and risk adjustment scores would not be understandable to patients without other population-level metrics that are proprietary to the health insurance providers. Moreover, quality information is generally already available to enrollees in the plans' web-based technologies. If third-party app developers wish to develop their own quality measures (which is inadvisable given the move toward alignment), calculate them, and display them for consumers, it can do so through accessing the basic claims information from health insurance providers and the clinical information for the health care provider APIs. Finally, while health insurance providers may have lab results, for example, as part of a prior authorization request, there is no guarantee that it is the most recent value or represents the complete picture of the patient's health, potentially causing confusion. Thus, we are unclear what information in the possession of health insurance providers and would be useful to consumers that is in the USCDI. We believe certain clinical information, such as step therapy status, would be valuable in the payer to payer communications for care coordination purposes proposed by CMS. **Sharing clinical information via the open API to third-party apps for the broad USCDI should not be required of health insurance providers, but rather sought from providers as the source of truth. CMS and ONC should work with health insurance providers to identify a subset of clinical information relevant to consumers.**

We understand that the Health Information Technology Advisory Committee (HITAC) chose not to include pricing information in the USCDI at this time recognizing there is a lack of stakeholder consensus in this area. We do not believe that pricing information, particularly granular level data, belongs in the USCDI—which is a clinical not administrative standard. In addition, for reasons we directly address in our response to the ONC's questions about including pricing information in the past, present or future as part of the definition of electronic health information (EHI) in the section of this letter addressing the information blocking provision, we oppose the public disclosure of granular level pricing data.

AHIP recommends ONC exercise its enforcement discretion to allow voluntary use of newer versions of any adopted standard by willing trading partners, without further rulemaking. We support use of the "Standards Version Advancement Process" to allow health IT developers to implement future versions of the USCDI faster than the regulatory cycle can accommodate. We appreciate ONC's effort to address the time-lag between the publication of a standard and its inclusion in regulation. Overall, the proposed process appears workable, and we suggest three additions:

1. We recommend ONC establish a mechanism for standards developers and implementers to submit candidate "new versions" for ONC consideration to an email address or a web site. The list of candidates should be publicly viewable prior to ONC's formal consideration.
2. We recommend that ONC seek public comment prior to rulemaking to incorporate input when it drafts a Proposed Rule.
3. We ask ONC to provide clarity on the timeline of changes, including a cut-off date for submission of new versions, a target date for ONC's NPRM, and a target date for publication of the updated Interoperability Standards Advisory (ISA). We recommend ONC develop and release a schedule for periodic review of new standards versions.

The proposal appears focused on highly modular standards/specifications such as HL7 FHIR. A similarly streamlined process would be extremely helpful for standards which do not have components updated

independently, e.g., NCPDP SCRIPT, ASC X12N, if only to address minor updates discovered during implementation and extended use of these standards. We understand that major updates, such as SCRIPT 10.6 to 2017071 may not be addressed by the proposed process. However, in these cases, ONC's compliance enforcement discretion for the use of updated standards between willing trading partners would encourage more innovation and efficiency across the health care sector.

§ 170.205(b) Electronic Prescribing

We appreciated CMS and ONC working together to ensure existing standards are relied upon where possible. **AHIP supports adopting the National Council for Prescription Drug Programs (NCPDP) SCRIPT 2017071 standard that will be effective January 1, 2020 for the 2015 Certification Criteria**, which will align the 2015 Certification Criteria with the CMS Medicare Part D e-Rx and MH standards.

§ 170.315(b) (10) Electronic Health Information Export Criterion

AHIP supports requiring health IT developers of certified health IT products to provide the capability to electronically export information for a single patient upon request or all patients when a provider seeks to change health IT systems. However, we recommend ONC align the definition of "electronic health information" used in this Certification Criterion to the same definition used in the information blocking provision.

As previously stated, CMS expects health plan-deployed APIs to meet standards comparable to the 2015 Edition criteria, though they do not need to be certified. With that in mind, believe it is unnecessary for health plan APIs to meet this criterion. As we note in our CMS comments, we do not believe that a patient-based or population-based export feature is necessary for health plans sharing information via APIs.

Health plans share information with providers as part of the treatment, payment, and operations (TPO) authority under HIPAA on a regular basis. For example, plans furnish large scale data sets and performance reports to accountable care organizations, medical homes, and as part of bundled payment programs. Moreover, many plans currently share with clinical providers as part of Health Insurance Exchanges (HIEs). Once the Trusted Exchange Framework and Common Agreement (TEFCA) is finalized, we anticipate even greater connections through the "network of network" the framework envisions.

ONC should allow these efforts to unfold. ONC should not dictate how insurance providers connect with providers. Patients will be able to use these APIs to transfer their information to third-party applications ("apps") of their choosing as part of the CMS rule. Consumers wishing to download the data themselves, and not to an app, can do so directly from the plan using the plan's consumer portal. **Therefore, we recommend CMS and ONC specify in the final rule that while health-plan deployed APIs are expected to meet standards comparable to 2015 Certification Criteria, they are not expected perform EHI export in the manner specified in this criterion.**

§ 170.315(d) (12) Encrypt authentication credentials

AHIP supports requiring health IT developers to attest to whether they encrypt authentication credentials as a criterion of 2015 Edition Certification. We support ONC's proposal to use an

attestation process for health IT developers who possess this functionality, and we recommend the ONC-Authorized Certification Bodies (ONC-ACBs) validate these attestations to ensure certified health IT products are executing the encryption functions they claim to possess. If ONC seeks to require other entities to implement this functionality in the future, we recommend ONC allow for additional time for entities to comply with the requirement, as entities will need time to ensure these standards can be accommodated without impairing information flow.

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

AHIP supports requiring health IT developers to attest to whether they utilize multi-factor authentication as part of 2015 Edition Certification Criteria, consistent with industry recognized standards (e.g., National Institute of Standards and Technology [NIST] Special Publication 800-63B Digital Authentication Guidelines, ISO 27001). We support ONC's proposal to use an attestation process for health IT developers who possess this functionality, and we recommend the ONC-Authorized Certification Bodies (ONC-ACBs) validate these attestations to ensure certified health IT products are executing the multi-factor authentication processes they claim to possess. If ONC seeks to require other entities to possess this functionality in the future, we recommend ONC allow for additional time for those entities to comply with the requirement, as they will need time to ensure that these standards can be accommodated without impairing information flow.

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

ONC proposes to replace the existing two data segmentation for privacy (DS4P) criteria with three new 2015 Edition DS4P certification criteria (two for C-CDA and one for a FHIR-based API) that would support a more granular approach to privacy tagging data and consent management for health information exchange supported by either the C-CDA or FHIR-based exchange standards. While we are open to evaluating "privacy tagging" in a variety of electronic environments, we remain uncertain how using a variety of "tagging" functions will support greater interoperability and make patient information more readily available at the point-of-care.

We are very concerned with any proposed adoption of a standard that moves the level of tagging for segmentation purposes from the document level to the level of individual data element. Any such requirement will not only create risks of detrimental system performance, as every data element captured will need to be individually tagged with metadata, but will also create significant burden on health care organizations to develop systems and processes that support segmentation at the data element. Such a requirement will also create the risk of having incomplete health records filled with data element holes (so-called "swiss-cheese effect"), which could increase the risk for medical errors and other patient safety issues, undermining care management efforts and clinical determinations. For example, tagging information can be suppressed or removed from an electronic record resulting in incomplete information being made available to individuals and their treating providers.

We also believe the standard for DS4P at the data element is not mature enough to warrant implementation. Although a DS4P implementation guide has existed since May 2014, the ISA still shows that adoption of this guide is low. The Consent2Share FHIR Consent Profile emerging implementation specification, which uses FHIR resources to represent and persist patient consent for

treatment, research, or disclosure, is still in development with feedback requested.[2] We also understand that Consent2Share does not appear to have a clear owner moving forward and is not a standard nor implementation guide that has gone through an SDO process. Based on the current status of DS4P-related implementation specifications, we feel it is premature of ONC to require this capability as part of 2015 Certification Criteria.

Getting legal and operational designations to mesh to the degree of precision necessary to enable patients to choose which segments of data to share will be contentious, laborious, and run counter to member expectations. For example, 42 CFR Part 2 attaches to records based on the provider, but other state laws may require health plans to filter substance use conditions at the diagnostic level, regardless of the source of the diagnosis. In addition, there is no standardized delineation of "mental health diagnoses," which the Mental Health Parity and Addiction Equity Act (MHPAEA) leaves up to state law or to health plans. Mapping such a distinction on to diagnostic or service codes would require a clinical standards development process, would probably fail to align with certain state laws and will create needless conflict across professional organizations. Inevitably, the distinction drawn whether for mental health or other conditions and services, will not line up with the specific expectation of the consumer.

If consumers are concerned that some of their PHI is too sensitive to share, they can rely on existing HIPAA-compliant mechanisms. **Consumers should have the choice to share all or none of their data. If consumers have concerns about specific information, they should be directed to the existing path to obtain information via other means (e.g. CD-ROM) that can be segmented based on their preferences.**

Finally, there are currently no, or very limited instances requiring data segmentation at the element level and building this capability for potential future policy development instances would be unwarranted. **AHIP does not support replacing the existing DS4P criteria with the proposed new 2015 Edition DS4P certification criteria at this time. We encourage ONC to conduct situational "use test cases" demonstrating how this functionality will be effectively used across a variety of environments prior to making this functionality effective.**

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

Please see our comments above regarding §170.31(b)(12) Data segmentation for privacy-send. **AHIP and our member plans are very concerned with any proposed adoption of a standard that moves the level of tagging for segmentation purposes from the document level to the level of individual data element for the same reasons enumerated above.**

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

AHIP supports adopting the consent management for APIs criterion in the 2015 edition Certification Criteria. Consent management is necessary for any access to a system with PHI. Consent management should be sufficiently robust to ensure patients are fully aware of the nature of the consent, including (i) identity of third-party recipients of disclosure; (ii) extent of information being disclosed; (iii) time limit on consent; (iv) restrictions on redisclosure by recipient; and (v) extent of the patient's rights regarding particular types of information (e.g., psychotherapy notes, or information re: involuntary psych

[2] https://www.healthit.gov/isa/data-segmentation-sensitive-information

holds). ONC should communicate with CMS, the HHS Office for Civil Rights (OCR), and the Substance Abuse and Mental Health Services Administration (SAMHSA) (which enforces Part 2) to address any potential conflicts between this certification criterion and their policies, including reconciliation with 45 CFR Part 2.

SECTION VII.B.4 – APPLICATION PROGRAMMING INTERFACES

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

ONC proposes to adopt a new API criterion which would replace the "application access—data category request" certification criterion and become part of the 2015 Edition Base EHR definition. This new "standardized API for patient and population services" certification criterion would require the use of Health Level 7 (HL7®) Fast Healthcare Interoperability Resources (FHIR®) standards and several implementation specifications. The new criterion would 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.

AHIP supports requiring health IT developers of certified health IT products to support API-enabled services for data on a single patient and multiple patients. We feel this certification criterion is appropriate in the context of facilitating clinical data export from EHRs. We note that health IT developers will need time and resources to build the technology and surrounding operation protocols needed to implement this criterion, especially for population-level queries. The current lack of a standard for implementing population-level queries could result in implementation of solutions that raise privacy concerns. In particular, we have significant concerns that certified health IT developers will implement different methodologies of varying maturity to match patients within the certified health IT to the patients listed in the population-level query. Each incorrect patient match represents a potential breach of protected health information, which could expose the health care provider implementing the API to potential liability under HIPAA. **We recommend that ONC assist in these efforts by releasing implementation guides and make such guides available in a sufficient amount of time for health IT developers to develop and test capabilities prior to implementation.**

We ask that ONC clarify that health care providers who choose not to implement the population-based query functionality would not be engaged in information blocking. We also ask that ONC clarify that health care providers that do elect to implement population-based queries have leeway under the privacy and security exceptions to information blocking to deny population-level queries if there would be issues in matching patients within the system to the list of individuals that the querying party requested, or other security concerns.

AHIP supports adoption of HL7 FHIR Release 4 as a regulatory base standard, however, we recommend ONC provide greater flexibility in adopting future FHIR Releases and associated implementation guides. We believe that ONC should accommodate updates to standards versions and implementation guidance without rulemaking. Changes or extensions to a standard named in regulation could complicate compliance, as rulemaking often lags innovation and improvement. Systems implementations should not be forced to forego new, improved versions because the regulation mandates use of an older version. To solve this issue, **we recommend providing sub-regulatory guidance for all implementation specifications of adopted standards, including all FHIR profiles, and allowing developers to update standards versions in accordance with the Standards Version Advancement Process with public input rather than requiring standards updates to go through the rulemaking process**

HEALTH IT FOR THE CARE CONTINUUM

Health IT and Opioid Use Disorder Request for Information

ONC seeks comment on health IT functionalities and standards to support the effective prevention and treatment of opioid use disorder (OUD) across patient populations and care settings. Specifically, ONC seeks comment on how the existing 2015 Edition certification criteria as well as proposals within the proposed rule for revised or new criteria support OUD prevention and treatment.

AHIP applauds ONC for exploring ways to advance health IT across the care continuum to support efforts to fight the opioid epidemic. Health insurance providers have leveraged health IT to improve adherence to opioid prescribing guidelines and to increase the safety of prescribing for controlled substances. We agree that improving access to data from disparate sources is critical to ensuring all health care stakeholders are able to play a meaningful role in this crisis.

AHIP recommends ONC consider two additions to the 2015 Certification Criteria to support OUD prevention and treatment: *Drug-Drug Interaction Checks for Computerized Order Entry* and *Care Plan Criteria* (under Care Coordination). Including the *Drug-Drug Interaction checks for computerized order entry* criterion could support efforts to prevent potentially dangerous co-prescribing such as prescribing opioids with benzodiazepines. Including the *Care Plan* criteria could better coordinate care for patients seeking treatment for opioid use disorders. Additionally, AHIP would support the development of additional informational guides and resources for OUD providers.

SECTION VIII – INFORMATION BLOCKING

Section 4004 of the Cures Act added section 3022 of the Public Health Service Act (PHSA) ("the information blocking provision"), which defines conduct by health care providers, and health IT developers of certified health IT, exchanges, and networks that constitutes information blocking. In this proposed rule, ONC proposes to interpret or define certain statutory terms and concepts, including electronic health information (EHI), health information networks (HINs), and other concepts.

§ 171.103 Information Blocking

AHIP supports ONC's efforts to promote efficient exchange of information between health care stakeholders and we support the intention of the information blocking provision. We agree steps must be taken to ensure "payers and other entities that purchase health care services can obtain the information they need to effectively assess clinical value and promote transparency concerning the quality and costs of health care services" (84 FR 7517).

We recommend ONC strengthen its position on information blocking by identifying processes that are "highly probable" to constitute information blocking rather than "likely" to constitute information blocking. In view of the penalties proposed, a broad interpretation of the existing definition of "likely" could create opportunities for exploitation of normal processes for patient signature or authorization for the release of EHI by health care organizations. We also recommend ONC provide additional examples of practices that are highly probable to constitute information blocking in the final rule. These examples should be linked to real-world experience, so stakeholders can better understand information blocking activities.

We also recommend third-party application developers be included in the list of Actors subject to the information blocking provision. As these applications are meant to be the mechanism through which health care stakeholders will utilize APIs, they are in a unique position to facilitate or impede exchange of information. They should be held to the same standard as health IT developers and other potential information blocking Actors.

We note the preamble states the information blocking provision may operate to require Actors provide access, exchange, or use of EHI in situations HIPAA does not. As the preamble explains, the HIPAA Privacy Rule permits, but does not require, covered entities to use and disclose ePHI in most circumstances. The information blocking provision, on the other hand, requires an actor to provide access to, exchange, or use of EHI unless they are prohibited from doing so under an existing law or are covered by one of the exceptions. It is possible an actor could take some action with the intention of complying with the information blocking provision that inadvertently does not coincide with HIPAA. As HIPAA violations carry significant penalties, **we recommend a safe harbor be added to HIPAA, which would insulate the entity from penalties/OCR enforcement, for entities acting in good faith to comply with the information blocking provision.**

We also recommend establishing a good faith exception within the information blocking provision for Actors who withhold data under the good faith belief that sharing the information in a specific circumstance would not comply with other federal or state laws. In addition to the good faith exception, we also urge ONC to establish other appropriate state law-based exceptions, as determined through collaboration with states, health care providers, and other stakeholders.

§ 171.102 Definitions

ONC proposes to further define or interpret certain terms or concepts that are present in the statute. **AHIP believes ONC's proposed definitions in relation to the information blocking provision are defined too broadly to be functional.** We recommend these definitions be narrowed to ensure the information blocking provision can be effectively executed in line with Congress' original intent in the 21st Century Cures Act. We also recommend that both CMS and ONC should, whenever possible, leverage existing HIPAA definitions to help ensure clarity and consistency, and build on the existing infrastructure and experience with HIPAA compliance. Refinements to these definitions should be put in place before any information blocking penalties are enacted.

Electronic Health Information (EHI)

The current definition of EHI encompasses far too many types of information to allow for reasonable compliance and actionable enforcement of the information blocking provision. Such a comprehensive definition of EHI will hinder an actor's ability to determine what does and does not constitute information blocking, resulting in the potential release of more information than is required and compromising privacy and security. The Cures Act does not define EHI, however, "EHI" has long been used by ONC and others as synonymous with electronic protected health information (ePHI).[3] For the purposes of this

[3] *E.g.*, *compare* 42 C.F.R. §495.20(d)(15), (f)(14) *with* §495.22(e)(1), (f)(1) (using the terms EHI and ePHI interchangeably in establishing the protect patient health information objective for meaningful use); 80 Fed. Reg. 62762, 62793 – 95 (Oct. 16, 2015) (using EHI and ePHI interchangeably and establishing requirements regarding

proposed rule, **we recommend the definition of EHI be limited to a subset of ePHI for which there are defined standards available for Actors subject to the information blocking provision. It should not include information that relates to the past, present, or future payment for the provision of health care to an individual.** ONC should work with stakeholders to update future definitions of EHI as new standards become available.

Both CMS and ONC should, whenever possible, leverage the HIPAA definitions and requirements that apply to HIPAA covered entities to help ensure consistency and promote understanding within the health care environments. Requiring adherence to two similar yet distinct electronic data definitions (EHI and ePHI) will cause confusion among information blocking Actors and increase the likelihood of violation of the provision. The healthcare industry is familiar with the definition of protected health information (and by extension, ePHI) and has developed policies and procedures around this definition for several years. Actors will be best able to comply with the information blocking provision using this established data definition, which will in turn make it easier for ONC to monitor and enforce the provision. While we recognize ONC's desire to define an expansive set of information that constitutes EHI, we feel expanding the definition of EHI beyond ePHI should occur in stages through an ongoing, iterative regulatory process to allow health care stakeholders to update their systems and processes accordingly. For example, ONC might consider expanding the definition of EHI to include electronically transmitted information that identifies or could be reasonably used to identify an individual, which is part of ONC's current EHI definition, in a future proposed rule. **We stress that any future expansion of the definition of EHI beyond the above definition should be subject to rulemaking.**

We also recommend ONC clarify that the definition of EHI only includes data collected on the consumer and not data that is generated. In other words, ONC should clearly state that the definition of EHI does not include data that is created through aggregation, algorithms, and other techniques that transform observational health information into fundamentally new data or insights that are not obvious from the observational information alone (e.g., population-level trends, predictive analytics, risk scores, quality measure results, and EHI used for comparisons and benchmarking activities).

Additionally, the definition of entities that can create or receive EHI includes both HIPAA-covered and non-HIPAA covered entities such as life insurance companies. **We recommend the definition of EHI be limited to HIPAA-covered entities**.

Health Information Network (HIN)

ONC seeks comment on whether the proposed definitions of information blocking Actors (including health care providers, health IT developers, health information networks [HINs], and health information exchanges [HIEs]) are broad enough (or too broad) to cover the full range of individuals and entities that could be considered health information networks within the meaning of the information blocking provision.

ONC proposed to define an HIN as an entity that "enables, facilitates, or controls the movement of information between or among different individuals or entities that are unaffiliated." This definition of an HIN is excessively broad and could include organizations that are not networks. For example, health

---

security of ePHI for the protect EHI objective); 68 Fed. Reg. 8334, 8334 (Feb. 20, 2003) (using EHI and ePHI interchangeably); 67 Fed. Reg. 53182, 53194 (Aug. 14, 2002) (describing EHI as a subset of PHI).

plans, technology companies that handle EHI, and standards developing organizations [SDOs] or organizations that develop recommended interoperability polices are not networks and could, inappropriately, be included in the proposed definition. Many entities could conceivably facilitate information exchange between other unaffiliated entities or individuals, many of whom may not actually possess shareable data themselves. Specifically, the definition as written could be construed as including payers, which was not Congress' intent for this provision. Congress initially intended the information blocking provision to primarily apply to health care providers and EHR vendors. Payers are not mentioned in the text of the Cures Act[4], the back versions of the bill[5], the associated committee report[6], or the transcript of the full Energy and Commerce Committee mark-up[7]. It is clear payers were never contemplated as Actors in the information blocking provisions of the Cures Act. This is further reflected in the proposed rule as ONC did not include payers in any of the HIN examples provided.

Furthermore, including health plans in the definition of HINs subject to the information blocking provision would be redundant with the existing information blocking enforcement mechanisms in their contracts with CMS as well as the provisions outlined in the companion CMS interoperability proposed rule. We request that ONC should provide further clarification as to what entities would and would not be considered HINs. **We strongly recommend ONC narrow the definition of "Health Information Networks" and clearly state in the regulatory text payers are not included in this definition and thus are not subject to the information blocking provision.**

Additionally, we recommend that ONC remove "substantially influences policies or agreements" from the first definition of a HIN ("an individual or entity that satisfies one or both of the following— (1) Determines, oversees, administers, controls, or substantially influences policies or agreements that define business, operational, technical, or other conditions or requirements for enabling or facilitating access, exchange, or use of electronic health information between or among two or more unaffiliated individuals or entities"). This removal will eliminate the possibility that two entities exchanging information for business purposes would be considered a HIN.

<u>Health Information Exchange (HIE)</u>

ONC proposes to define an 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." AHIP feels the definition of HIE is also excessively broad. The fact the definition of an HIE includes individuals is difficult to understand and, as with the HIN definition, could be misconstrued as to include individuals or organizations that are not actually HIEs.

We feel it is unnecessary to separately define HIN and HIE as two different terms. The two definitions overlap and appear to be broad enough to have the information blocking provisions apply to vendors and networks that provide such exchange services. Two separate definitions of terms that overlap to this extent will create unnecessary confusion in interpreting and applying these terms.

---

[4] 21st Century Cures Act, Pub. L. No. 114-255, 1033 Stat 130 (2016)
[5] H.R. 6, 114th Cong. (2015)
[6] H. Rep. No. 114-190 (2015)
[7] Markup of H.R. 6, 21st Century Cures Act, Tuesday, May 19, 2015 House of Representatives, Committee on Energy and Commerce, Washington, D.C.

ONC should define HIEs as a subset of HINs, combining the two types of Actors in one combined definition. If these two concepts are not combined, ONC should provide additional clarification regarding the difference between an HIN and an HIE and provide additional examples showing the difference between the two concepts. **We recommend ONC define HIEs as a subset of HINs. Barring that combination, ONC should provide further clarification on the definition of an HIE. ONC should also clearly state payers are not included in the definition on an HIE and thus are not subject to the information blocking provision.**

Health Care Provider

ONC proposes to adopt the definition of health care provider used in section 3000(3) of the PHSA, noting this definition is different from the definition of "health care provider" under the HIPAA Privacy and Security Rules. ONC is considering adjusting the information blocking definition of "health care provider" to cover all individuals and entities covered by the HIPAA "health care provider" definition. **AHIP recommends the definition of "health care provider" cover all individuals and entities consistent with the HIPAA definition.** The information blocking provision is complex and a consistent definition for health care providers will help decrease confusion and help the agency identify specific situations where a provider may need help understanding "information blocking," thereby promoting compliance in a proactive fashion.

Price Information

ONC seeks comment on the parameters and implications of including "past, present and future" price information within the scope of EHI for purposes of information blocking. Recognizing the definition of EHI does not directly impact insurance providers that are not subject to information blocking, we provide comments below as it interrelates with the CMS proposed requirements to share paid claims and to the extent health plans and health care providers must work together to ensure consumers have the information they need at the right time and place to make health care choices for themselves and their family.

AHIP and our members are firmly committed to providing consumers greater price transparency to aid in their decision-making and empowering them to choose health care services that are both affordable and right for them. Health plans offer transparency tools that give consumers estimates of anticipated costs and ways to compare services based on price, quality, and accessibility. Health plans recognize that existing tools require additional features and information from providers to allow for pre-service comparison shopping not currently available for some services. As an industry, we continue to innovate and lead the way in giving our members useable, practical, and understandable information to aid in their decision-making. **As ONC develops its final rule,** we urge consideration of the unintended consequences of the release of granular pricing data on the progress private-sector health insurance providers have already made to provide tools and convey useful information. **to consumers.**

While we all agree consumers should be empowered to shop for health care and make their own decisions, this has not traditionally been the case. Efforts to increase health literacy, share where and how to access information, and encourage incorporating the information into health care choices will benefit everyone. **ONC and CMS should work with stakeholders in a public-private partnership to harness ongoing innovations to ensure consumers have the prospective pricing and other information they need rather than creating a federal.**

Moreover, shoehorning prospective price estimates in the definition of EHI in order to include it within information blocking is not substantiated by the underlying legal authority. HIPAA addresses availability of retrospectively provided service information to consumers and does not require prospective estimates be offered. The 21st Century Cures law provisions on interoperability focus on sharing information included in the clinical record. **We do not believe ONC has the authority to mandate prospective pricing estimates as part of EHI.**

Price Information for Consumers

As ONC considers ways to encourage greater price transparency, it is important to recognize meaningful transparency for patients means understanding the expected costs for them individually and should consider not just price but quality and accessibility. As decisions in health care are most often made by the patient in concert with their health care providers, it is imperative that providers share responsibility for disclosing information and participating in decision tools.

Providing information on the relative cost and quality of a service for relevant providers can empower consumers to choose the high-value provider right for them. However, this information is most relevant when included as part of shared decision-making between the consumer and the referring physician. There may be clinical implications to the choices that need to be explained to the consumer or alterations to the care plan that need to be made based on the consumer' feedback. For example, cost-conscious consumers may find the out-of-pocket costs for a drug is too high necessitating the provider determining the best alternative. In such a case, shared-decision making based on this information could increase the likelihood of medication adherence. These choices can have a positive effect on health care spending and on consumers health outcomes. We are concerned that solely providing pricing information in absence of information about quality and accessibility, could have unintended consequences for consumers. Providers are in the best position to provide this context in partnership with consumers and their health plans, and **we urge ONC and other regulators to seek ways to engage the provider community in shared decision-making around costs.**

We stress the important difference between the price of a service and the consumer's cost associated with a service. Consumers are often not paying the full price of a service as a function of health insurance, thus, providing this information would not be useful to their decision-making process and could confuse consumers. What matters to patients is their out-of-pocket costs based on their specific health insurance. Even in displaying out-of-pocket costs, ONC must be careful to ensure competitively sensitive information is not provided, as we discuss below. **If ONC includes price estimates in future versions of the USCDI or a future definition of EHI, it should focus on consumer out-of-pocket costs displayed in a fashion that does not divulge trade secrets,** as discussed in the following section.

We recognize health care treatment decisions are often made in partnership between patients and their providers using a variety of information including cost, quality, location, language spoken, provider recommendation, and other factors. In many instances, there may only be one treatment option available and patients are most likely to follow the instructions of their health care provider. In other circumstances, services can be quite 'shoppable.' These shoppable services (e.g., MRIs) are the most relevant to the patient and present an opportunity to test price transparency changes. We urge ONC in developing any further regulatory actions on these issues to consider incremental changes that can test the effectiveness of including new elements of price information in EHI (e.g. defined services). **We recommend ONC begin any changes to price information and EHI with defined services most shoppable by consumers.**

Health plan cost-comparison tools often provide factors beyond costs essential to making the best decisions for a patient's individual needs. These considerations include the quality and location of network providers under a members' benefit. We recognize these decisions are made in partnership and patients most often follow the recommendations of their health care providers with greater priority than cost considerations. By engaging providers with ample information on price and quality, including comparisons of different treatment options, rather than solely the cost of the same drug or procedure, providers may be able to recommend multiple treatment options for a patient to consider (e.g., one inpatient and one outpatient) that have varying costs and other considerations such as risk of complications or time involved. These comparisons are critical to ensuring patients are empowered to choose the best health services at the right price for them. **We urge ONC to consider the variety of factors consumers use when making health care decisions, including provider quality information and treatment options.**

Recognizing patient costs do not exist in a vacuum and are dependent on several factors, efforts to furnish such information will need to begin with the type of plan in which the patient is enrolled. If a patient is subject to co-insurance rather than a co-pay, for example, the information that would help them decide would vary. This is part of the reason out-of-pocket costs are more important to patients than unit prices. Similarly, the patient's financial obligation can vary throughout the year depending on the structure of their plan. For example, a patient who has met their deductible and/or paid the plan's out-of-pocket maximum, would require far different information and advice with respect to costs than a patient who has not. Health plan tools provide patients with costs in context based on their benefit plan and in-network providers. Further, transmitting this information as part of EHI must reflect the current (real-time) status of their financial obligations such as the amount paid thus far under the deductible. As with all aspects of these disclosures, caveats abound, and patients must know these are estimates, rather than binding quotes. While there is a HIPAA transaction code set to allow providers to determine this information, providers often default to phone and fax communications. Significant resources would need to be invested in FHIR-based standards to allow an electronic exchange of such information via open APIs as an alternative. **We urge ONC to work with stakeholders to ensure future proposals consider the impact the type of plan in which a patient is enrolled and where the patient is in their benefit structure, so information provided to patients and consumers is the best reflection of the price they would pay.**

Price Information and Providers

Requiring public disclosure of pricing data could have potential negative competitive effects that could hinder fair negotiations and drive up prices. According to the Federal Trade Commission (FTC), "…transparency is not universally good. When it goes too far, it can actually harm competition and consumers. Some types of information are not particularly useful to consumers, but are of great interest to competitors."[8] Negotiated payment rates, including those delineated by billing codes for individual providers and plans, would unbalance leverage during negotiations, hinder market competition, increase prices and are inconsistent with existing Medicare Advantage and Part D non-interference statutory frameworks.[9] There are other ways to provide useful information to consumers without disclosing contracted information or trade secrets. This could include, for example, providing composite value scores comprised of cost, quality and patient experience information, where the negotiated amount cannot

[8] Koslov, T. and Jex, E.; *Price transparency or TMI?;* Federal Trade Commission Blog; Jul 2, 2015 2:31PM; https://www.ftc.gov/news-events/blogs/competition-matters/2015/07/price-transparency-or-tmi.
[9] 42 U.S.C. 1395w-111(i); 42 U.S.C. 1395w–24(a)(6)(b)(iii).

be backed into like co-insurance. Should disclosure of private contract negotiations be required, the cost impacts could be significant, causing serious disruption to our health care system to the detriment of consumers. **ONC should ensure any proposal related to pricing information protects market negotiations between health plans and providers.**

Practical considerations, such as the technology infrastructure, should also be part of ONC's future proposals. Any proposal would require significant coordination between health insurance providers and health care providers to determine the best method of transmission, whether that be a HIPAA transaction code set or an open API, for the information necessary for each party to develop an estimate. Providers know the array of services provided, while the plans know the coverage and payment rules. For price transparency to have a meaningful impact, estimates would need to be made widely available using a standard framework to allow easy and accurate comparisons between providers. Ultimately, estimates at the overall encounter level would be more helpful than the individual service. Infrastructure would need to be developed to give health insurance providers or health care providers the ability to run a claim pre-service or estimate a price respectively. **ONC should consider the means of relaying price information and work toward a standard framework for displaying service value and comparing prices between entities in future proposals.**

Information to Reduce Surprise Medical Bills

We believe making price information of provider and facility services more readily available to patients could have a positive impact on reducing and preventing surprise medical bills. Surprise medical bills result from the lack of participation by certain medical providers in a health plan provider network, often specific providers people do not actively choose or seek services from (anesthesiologists, radiologists, etc.). Addressing the arbitrary bills out-of-network providers send to patients, by reining in the maximum permissible bill amounts and encouraging greater network participation, will be most effective in preventing future surprise medical bills; however, this approach would require new federal or state legislation (in some states). **We recommend ONC consider ways in which price information can help prevent against surprise medical bills in future proposals.**

New requirements to create a single medical bill encompassing all facility and doctor services would fundamentally change hospital billing practices today. A single bill from a health care facility could certainly reduce surprise medical bills but would require new contractual relationships between facilities and providers. We are concerned the combination of facilities and providers would unbalance negotiation leverage in a way that facilities would increase prices for patients. As an alternative, ONC can consider how health care providers can work to ensure patients are matched with medical specialists in the patient's health insurance network.

Additionally, providing consumers with a binding quote prior to a healthcare service creates additional challenges. Even for scheduled care, particularly when providers are out-of-network and plans are unaware of their charges, a binding quote is not possible. As with other aspects of conveying anticipated costs, an estimate is all that is available currently. The industry would like to advance to a point where collaboration between health plans, facilities, and providers make binding quotes possible, but that is not the reality in the current environment. **We believe the single bill approach and provision of a binding quote would both be infeasible at this time. ONC should engage stakeholders in additional conversations on this topic.**

Providing detailed notice to patients about billing practices and expectations is, we believe, prudent and consistent with our view that patients are entitled to as much information about their care as possible. However, we note that information supplied to patients should be for notification purpose only, rather than a means of consenting to out-of-network charges of which the patient would be unaware. We support approaches to preventing surprise medical bills that address the root cause and have the potential to lower the cost of care for all. The query posed about ensuring all health care providers in an in-network facility charge the in-network rate would prevent most surprise bills while reining in the costs certain specialty providers charge. We believe this approach would likely reduce costs to the system; however, this would need to occur through a statutory change. **We recommend ONC support policies that address the source of surprise medical bills and lower costs by ensuring all health care providers at an in-network facility charge the in-network rate.** In addition, ONC should work with the hospital community to determine how facilities can use technology to match patients to in-network physicians.

Future Considerations

We feel the definitions used in the information blocking provision should be clarified to narrow their scope. **If ONC decides to expand these definitions in the future, we recommend ONC work with stakeholders to establish appropriate definitional parameters and a realistic operational timeframe.** For example, we recommend the definition of EHI be limited to ePHI in the final rule. If ONC expands that definition, the effective date should be sufficiently after the rules effective date to allowing for ample time for implementation as Actors will need time to adjust their technology and practices accordingly.

SECTION VII.D – PROPOSED EXCEPTIONS TO THE INFORMATION BLOCKING PROVISION

In this proposed rule, ONC identifies several reasonable and necessary activities as exceptions to the information blocking definition, each of which it proposes would not constitute information blocking. The exceptions would extend to certain activities interfering with the access, exchange, or use of EHI but that may be reasonable and necessary if certain conditions are met.

AHIP supports this exception to the information blocking provision. We agree there are certain instances where an actor might reasonably need to restrict electronic access to data. We note that the proposed exception requires organizations to develop and implement new written policies and procedures to determine the existence of an information blocking violation, which will create a significant burden and added complexity for existing privacy processes. This burden is exacerbated by the broad definition of information blocking practices. As proposed, the definition of information blocking practices does not consider exfiltration of information that 1) may occur without a consumer's knowledge or 2) that exceeds the limits authorized by the consumer. Either type of exfiltration counter to the consumer's knowledge may be intentional or may be a consequence of inadequate consumer notification by the vendor about what will be accessed, how that information will be used, and whether secondary/tertiary uses will or can be made of the information without further informing the consumer and/or seeking permission. **We recommend ONC narrow the proposed definition of information blocking practices and clearly identify reasonable and necessary activities that do not constitute information blocking.**

As stated in our comments on the previous section, health plans are not included in the definition of Actors subject to the information blocking provision, as they are neither health IT developers of certified health IT, health care providers, health information networks, or health information exchanges. However,

we feel there are reasonable and necessary circumstances in which a health plan may need to deny or delay a request to share data by a consumer that are in line with ONC's exceptions to information blocking. CMS and ONC should work together to establish similar exceptions for payers and providers, respectively.

For example, ONC proposes an actor may engage in practices or implement measures protecting the privacy or security of electronic health information. We feel an insurance provider should also have the ability to restrict access to information transmitted via APIs if the manner in which the information is accessed, exchanged, or used is not permitted under the HIPAA Privacy Rule, or if the access, exchange, or use would compromise the confidentiality, integrity, and availability of the information. We may have sufficient reason to be concerned a third-party app developer has malicious intentions and, therefore, would want to delay connection until due diligence can be completed. As another example, an insurance provider can deny a request that is infeasible, or temporarily make the systems unavailable for maintenance. **We recommend CMS similarly identify and include in the final rule circumstances in which it may be appropriate for insurance providers to delay or deny a request by a consumer via a third-party app developer.**

§ 171.201 Exception – Preventing harm

AHIP supports this exception to the information blocking provision. **We suggest that the focus on physical harm in the determination by a licensed health care professional that disclosure of EHI is reasonably likely to endanger the life or physical safety of a patient or another person is too narrow and should be expanded to include psychological and other forms of non-physical harm**.

§ 171.202 Exception – Promoting the privacy of electronic health information

AHIP supports the exception to the information blocking provision for promoting the privacy of EHI. As currently defined in the Proposed Rule, however, the privacy exception would require significant administrative complexity to implement. For example, in order to meet the "pre-condition not satisfied" sub-exception, the actor not only needs to have written policies and procedures in place concerning the federal or state privacy pre-condition, but must also do "all things reasonably necessary within its control to provide the individual with a meaningful opportunity to provide" a consent or authorization to share the information. **We believe that Actors should be permitted to decide that it would be too burdensome to seek multiple consents or authorizations to share EHI at the request of a third party.** For example, if a case management service requests access to EHI pertaining to multiple patients' substance use disorder treatment, the health care provider should not be penalized for deciding that it would be too difficult to seek consent or authorization from each applicable patient to share EHI with the case management service provider.

Even when consent is obtained, we note that the industry lacks the capabilities to validate that an entity has the appropriate access credentials. While we support invoking this exception when an individual doesn't want to share their information, a back-end solution to document their choice does not yet exist. **We recommend that ONC work with industry stakeholders to develop the technological capabilities needed to document use of this exception**. This should include clarification as to whether an actor would need documentation of an individual's blanket permission to share or not share data (that the individual could change at will) or of each discreet request every time information is requested.

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

We are also concerned the proposed exception does not sufficiently recognize bad Actors currently present in the environment (for example, organizations that employ security-related attacks on other organizations or those that may have received authorization to access data but may collect more than authorized or use the information in unauthorized ways). It is essential this exception enables Actors to address the range of such security threats.

Lastly, **we recommend ONC provide additional clarity regarding the complexities and challenges of separating out and restricting access to *42 CFR Part 2* data from other EHI (e.g., when the information is contained in clinical notes).**

§ 171.203 Exception – Promoting the security of electronic health information

AHIP supports the exception to the information blocking provision for promoting the security of EHI. We believe this exception is needed to promote proactive steps toward fixing security risks, while improving public trust. The Proposed Rule would require developers of certified health IT to share EHI with third party applications of a patient's choice through APIs. These third-party application developers, which are entering the healthcare market at a rapid pace, are often not covered by HIPAA because they offer their applications directly to consumers and not on behalf of a health care provider or health plan. We recommend ONC and HHS to take additional steps to ensure a thoughtful approach to how Actors, who are the for the most part covered by HIPAA as covered entities or business associates, share EHI with these non-HIPAA entities, and ensure that such third-party applications are equipped to handle EHI. **We recommend ONC update this exception to indicate, in addition to delaying access to data, an actor's attempts to thoroughly and sufficiently vet external locations of exchange (e.g., third party applications, networks) prior to sharing EHI does not constitute information blocking.**

In addition to this exception, we feel that requiring certification and vetting of third-part applications would be an important step toward combatting potential security risks. The proposed rule currently contains no certification process for third-party apps. Given the access to personal health information these apps are expected to have and the potential privacy risks they pose, **we recommend that a process be implemented by the Federal Trade Commission (FTC) to vet apps for the adequacy of the consumer disclosures, the privacy and security of the information once it is no longer governed by the HIPAA and secondary uses are permitted, and clinical soundness (for those applications that offer medical advice).** The vetting process should be at the application and application developer level,

not just at the entity level, and the results of such vetting process should be made public in the form of an application "safe list." Additionally, Actors should be able to refuse to share information with non-vetted applications.

In addition to the current consumer complaints process and to enhance oversight, we further recommend the establishment of a process for health plans and providers to submit complaints to the FTC about apps that are suspected of misleading consumers, misusing personal health information or otherwise failing to meet basic standards for privacy and security of personal health information. **After evaluation of complaints, the FTC should publicly post a list of apps that do not meet basic standards to avoid continued provision of data to these developers without true understanding by the consumers of the heightened risk.**

Lastly, ONC should also update this exception to specifically permit Actors to share information about security threats with other Actors. Such language could improve and streamline security assessment across multiple Actors and would help less resourced Actors more efficiently target security improvements.

§ 171.204 Exception – Recovering costs reasonably incurred

AHIP supports this exception to the information blocking provision. However, we are concerned that this exception has the potential to be over utilized and recommend ONC monitor this exception closely to avoid abuse. We note there is a cost associated with making any initial or ongoing investment in health IT, and not all expenditures should be used to claim an information blocking exception. This exception has the ability to change revenue models, which could create gaming (for example, a health IT developer offering a product for free as a means of bypassing the provision). ONC should clearly define the types of cost recovery that are reasonable so cost recovery is not used as an excuse to slow exchange of information. ONC should also develop a more detailed definition of "fair market" and provide further guidance on how the term should be used (e.g., specifying a methodology or amount). **AHIP urges ONC to develop a process for information blocking Actors to routinely report their use of this exception, including specific timeframes for Actors to submit information to ONC and for ONC to determine whether the exception can be applied in a specific circumstance.**

We support ONC's proposal to exclude costs that are speculative or subjective or associated with electronic access by an individual to their EHI from this exception. However, we are concerned about extending this exception to an individual's "personal representative, agent, or designee," particularly the reference to "designees." The data accessed in this way by commercial "designees" (e.g., third party applications) has economic value, with costs associated with its provision. Prohibiting recovery of costs from designees (as opposed to the individual) as part of the information blocking provision, beyond API certification requirements, could reduce investment in interoperability capabilities and overall availability of information. It will also increase costs for API data providers such as providers and plans, who may have to shift these costs to patients. Additionally, one cannot assume a designee requesting EHI means the designee is acting on a direct order from an individual. We feel there is a difference between a patient consenting to having their information shared generally and a patient actively requesting their information be shared in a specific circumstance. We agree patients who actively request to share their information should not incur a fee, however, **we recommend requests based on a patient's general consent should not be included in this exception.**

§ 171.205 Exception – Responding to requests that are infeasible

AHIP supports this exception to the information blocking provision. However, we feel the language defining this exception is excessively vague, which could create uncertainty as to whether claiming this exception will ultimately be accepted by regulators and thus lessen its benefit. For example, we feel that the term "requisite technological capabilities" leaves too much room for interpretation and exposes a potential loophole to be "gamed" by the industry, and we recommend this language be changed to "requisite technological infrastructure or requirements." **We recommend ONC provide clear definitions of the terms used in this exception (e.g., timely, burdensome, etc.).** We would welcome the opportunity to further engage with ONC to develop appropriate definitions for these terms.
We recommend ONC update this exception to include additional examples of requests considered infeasible, recognizing infeasibility can come from the scale effects of requests for access in addition to the marginal cost of meeting any given request, or a lack of technical capability in production to meet a request. **We also recommend ONC clarify whether a request can be deemed infeasible if there is another widely accepted alternative for performing the same or comparable action.**

§ 171.206 Exception – Licensing of interoperability elements on reasonable and non-discriminatory terms
AHIP supports this exception to the information blocking provision. We recommend ONC simplify this exception and, provide additional guidance on the use of reasonable and nondiscriminatory terms (RAND) licensing, and its implementation. ONC should clarify what is considered "reasonable," and by whom. Given the extensive use of licenses as one element of commercial health IT software offerings, **we recommend ONC clarify which software licenses would be required to meet this exception to avoid information blocking and which would need to be revised to meet the provision.**
We further recommend ONC clarify its definition of "royalty" and which fees associated with licenses software would be considered a royalty and which would not, and hence only eligible for the exception for recovering costs reasonably incurred. We also recommend ONC clarify whether, in all cases, fees associated with software are also eligible for the cost recovery exception.

§ 171.207 Exception – Maintaining and improving health IT performance

AHIP supports this exception to the information blocking provision. We note there is a difference between planned and unplanned maintenance downtime. We agree it is desirable for service level agreements (SLAs) to address planned maintenance downtime; however, unplanned downtime due to circumstances beyond the information blocking actor's control may not be addressed in the SLA. In general, scheduling downtime is very complex even within an organization. Requiring the assent of every party affected by unplanned downtime will make needed system maintenance and upgrades more difficult to accomplish, threatening overall system quality. In addition to accounting for unplanned outages/downtime that affect information sharing, ONC should ensure that this exception accommodates circumstances when planned outages run significantly longer than anticipated, but for no longer than necessary to achieve the health IT maintenance or improvement objectives. **We recommend ONC adjust this exception to allow for greater flexibility in maintenance downtime situations.** Additionally, we recommend ONC develop an implementation guide outlining parameters of what is considered acceptable and unacceptable maintenance and applicable outage timeframes. We recommend this guide use the same language and parameters for all Actors.

Request for Information on a potential additional information blocking exception for complying with the Common Agreement for Trusted Exchange

ONC is considering proposing a narrow exception to the information blocking provision in future rulemaking for practices necessary to comply with the requirements of the Common Agreement. Overall, we support ONC's effort to establish a network-of-networks policy framework for trusted exchange of health information and its inclusion as a quality improvement activity for purposes of MLR requirements. We agree more needs to be done to encourage trusted exchange of health information through interoperable systems to support care coordination, care management, and population health.

Over the past several years, AHIP has engaged in discussions with the ONC on a wide range of health information technology issues. Pursuant to the 21st Century Cures Act, the ONC outlined a set of principles for trusted exchange and minimum required terms and conditions for trusted exchange in the DRAFT Trusted Exchange Framework and Common Agreement (TEFCA). Any provisions related to trusted exchange will likely need to be updated after the TEFCA is finalized. **Given the DRAFT TEFCA has not yet been finalized, we recommend ONC wait for the Common Agreement to be finalized before addressing this issue.**

REGISTRIES REQUEST FOR INFORMATION

Health IT Solutions Aiding in Bidirectional Exchange with Registries

ONC is seeking information on how health IT solutions and the proposals throughout this rule can aid bidirectional exchange with registries for a wide range public health, quality reporting, and clinical quality improvement initiatives.

AHIP supports efforts to facilitate bidirectional exchange of health information with registries. We support a standards-based approach to this exchange and recommend use of FHIR Release 4 standards for this purpose. We feel FHIR would be the most appropriate standard for data exchange with registries, as it allows the user to limit data sharing to only a patient's relevant data elements (as opposed to the C-CDA format with facilitates sharing of the entire patient record). However, we recommend ONC not designate specific implementation guidance using a regulatory or sub-regulatory process and instead utilize the Standards Version Advancement Process outlined in previous sections of the proposed rule for any future FHIR releases used for this purpose.

PATIENT MATCHING REQUEST FOR INFORMATION

ONC seeks comment on additional opportunities that may exist in the patient matching space and ways that it can lead and contribute to coordination efforts with respect to patient matching. Accurately identifying and matching patient records across payers and providers is a foundational element to ensuring patient privacy and maintaining data security. In the companion proposed rule, CMS acknowledges the considerable stakeholder feedback that the lack of a UPI inhibits interoperability efforts. We understand the constraints in accurately identifying and matching patient records across providers and payers absent a unique, standard identifier. This often includes attempting to match patient identity using a number of data elements to match along different degrees of certainty and still results in overall low match rates within and between entities.

ONC seeks input on specific patient matching solutions and authority for such requirements. specifically, HHS requests input on requiring a patient matching algorithm, a particular patient matching software, or expanding recent Medicare ID efforts by assigning an identifier to patients enrolled in federally regulated plans. **We recommend HHS not require a patient matching algorithm or a patient matching software solution**. Such federal requirements could result in overly prescriptive requirements that constrain iterative improvements in patient matching by the private sector. These solutions would not be able to keep pace with private sector solutions. Further, while assigning identifiers to patients enrolled in Medicare plans, Medicaid and CHIP, and QHPs in the FFEs would expand the number of patients with a CMS-wide identifier, it would not provide a solution for the millions of Americans who gain coverage through their employers or buy individual coverage outside of the FFEs. We do not believe the specific solutions contemplated in the RFI would sufficiently address patient matching challenges or support private sector innovation.

We strongly encourage HHS to continue to facilitate private industry innovation to advance patient matching solutions rather than adopting federal requirements. We believe the role of CMS and ONC is to convene industry stakeholders to collaborate on the goals and means for developing solutions to patient matching. This may include exploring best practices related to patient matching and improving matching criteria and setting a minimum floor for error rates. For example, ONC should work with CMS to advance standardization of demographic information such as applying the U.S. Postal Service standard to addresses or adding new data elements like email address.

Recently published research in the *Journal of the American Medical Informatics Association* funded by the Pew Charitable Trusts revealed that the standardization of address to the standard employed by USPS would improve match rates by approximately 3 percent, while standardizing last name to the standard used by the Council for Affordable Quality Healthcare would further improve match rates up to 8 percent.[10] These findings suggest match rates could be further improved if ONC required use of USPS standards for address within the USCDI and if ONC and CMS required use of USPS address standards by health care organizations. Consistent with Pew's recommendations related to improving patient matching, we further recommend CMS work with ONC to require other demographic information such as email address, mother's maiden name, or health insurance provider identification number in order to further improve match rates.

AHIP further recommends that ONC or CMS-convene a working group to identify minimum assurance rates which would vary by setting. For example, the level of assurance of accurate patient matching needed for administrative or payment information would be lower than the level of assurance needed for treatment. We additionally recommend CMS adopt a safe harbor for entities that follow best practices or meet these assurance rates. Industry should have the flexibility to continue to iterate solutions to identify and match patient records. Building on best practices or minimum assurance rates, such solutions may include leveraging patient authorization, improving existing processes like copying and storing a patient's ID card at the provider's office, or public-private partnerships like those that have successfully solved person-matching issues in other industries such as the airline industry and TSA security check process. We believe ONC' role is to facilitate and set a floor for such innovation, but not restrict private sector solutions.

---

[10] Shaun J Grannis et al., "Evaluating the effect of data standardization and validation on patient matching accuracy," Journal of the American Medical Informatics Association 26, no. 5 (May 2019): 447–456, https://doi.org/10.1093/jamia/ocy191