hfma
healthcare financial management association

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

CMS-9115-P

On February 22, 2019, the Centers for Medicare & Medicaid Services formally released a proposed rule on interoperability and patient access to health data. Under the proposed rule, Medicare Advantage (MA) plans, state Medicaid and Children's Health Insurance Program (CHIP) agencies, Medicaid and CHIP managed care plans, and qualified health plans (QHP) issuers in the federally-facilitated exchanges (FFEs) would be required to meet certain requirements regarding patient access to their health care information, including requirements related to application programming interfaces (APIs). Among other issues, the rule proposes public reporting related to provider attestations regarding information blocking. The proposed rule also includes Requests for Information (RFIs) related to advancing interoperability across the care continuum and improving patient matching. This rule is scheduled to be published in the Federal Register on March 4, 2019. **The public comment period ends on May 3, 2019**.

Simultaneous with the publication of this proposed rule, the Office of the National Coordinator for Health Information Technology (ONC) of the Department of Health and Human Services (HHS) issued a related proposed rule "21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program," which would implement certain provisions of the 21st Century Cures Act (P.L. 114-255), including conditions and maintenance of certification requirements for health information technology (health IT) developers and modifications to ONC's 2015 Edition health IT certification criteria.

Because this proposed rule cross references certain material from the ONC proposed rule, two Appendices to this summary relate to the ONC rule. Appendix A is a summary of the ONC proposed technical requirements with respect to APIs, and Appendix B is a summary of that proposed rule's requirements with respect to information blocking.

Table of Contents

I.	Background	2
II.	Technical Standards Related to Interoperability	3
III.	Patient Access Through APIs	8
IV.	API Access to Published Provider Directory Data	14
V.	Health Information Exchange and Care Coordination Across Payers: Establishing a Coordination of Care Transaction to Communication Between Plans	15
VI.	Care Coordination Through Trusted Exchange Networks: Trusted Exchange Network Requirements for MA Plans, Medicaid Managed Care Plans, CHIP Managed Care Entities, and QHPs in the FFEs	17
VII.	Improving the Medicare-Medicaid Dually Eligible Experience by Increasing the Frequency of Federal-State Data Exchanges	18
VIII.	Information Blocking Background and Public Reporting	20
IX.	Provider Digital Contact Information	21

X.	Revisions to the Conditions of Participation for Hospitals and CAHs	22
XI.	RFI on Advancing Interoperability Across the Care Continuum	24
XII.	Advancing Interoperability in Innovative Models	25
XIII.	RFI on Policies to Improve Patient Matching	26
XIV.	Regulatory Impact Analysis	27
	Appendices: Selected Sections of the ONC Proposed Rule	28
	Appendix A. ONC Proposed Rule: VII.B.4. Conditions and Maintenance of Certification: Application Programming Interfaces	29
	Appendix B. ONC Proposed Rule: VIII. Information Blocking	46

I. Background

In this proposed rule CMS aims to use its authority to advance interoperability and patient access to health information. The agency says the key "touch points" of the rule are:

- Enabling patients to access health information electronically without special effort through APIs.
- Ensuring that providers have access to information on patients regardless of where they previously received care by preventing providers from inappropriately restricting the flow of information to other providers and payers.
- Ensuring that payers make enrollee electronic health information available through an API.
- Making it easy for patients and providers to identify providers within a plan's network.

The history of HHS efforts to promote interoperability of electronic health records is reviewed. This includes provisions of the 2017 Executive Order 13813 to Promote Healthcare Choice and Competition Across the United States and the myHealthEData initiative as well as a variety of activities dating back to the 2004 creation of the Office of the National Coordinator for Health Information Technology (ONC) and the 2009 enactment of the Health Information Technology for Economic and Clinical Health (HITECH) Act (P.L. 115-5). CMS also discusses its work with private partners, such as participation in the Da Vinci project led by Health Level 7 (HL7), a standards development organization.

Challenges and barriers to interoperability are described, which CMS identified through stakeholder meetings, comments received on RFIs, through letters and during rulemaking. The major barriers are the lack of a unique patient identifier (the subject of an RFI in section XIII below); the lack of standardization in the interface technology and the underlying data, particularly with respect to APIs; information blocking; the lack of adoption of certified health information technology among post-acute care providers; and the lack of alignment between federal and state privacy and security standards.

II. Technical Standards Related to Interoperability

In this section of the proposed rule CMS describes the framework and general approach it has taken in proposing the specific standards for MA organizations, state Medicaid and CHIP agencies, Medicaid and CHIP managed care organizations, and QHP issuers in the FFEs (referred to collectively in the preamble to the rule as "payers") that are set forth in section III.C, summarized below.

A. Technical Approach and Standards

For purposes of this proposed rule, CMS uses the definition of *interoperability* that appears in section 3000 of the Public Health Service Act (as amended by the 21st Century Cures Act):

> The term "interoperability", with respect to health information technology, means such health information technology that-
>
> (A) enables the secure exchange of electronic health information with, and use of electronic health information from, other health information technology without special effort on the part of the user;
>
> (B) allows for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable State or Federal law; and
>
> (C) does not constitute information blocking as defined in section 300jj–52(a) of [the Public Health Service (PHS) Act].

CMS states that a core policy principal in the proposed rule is that "...every American should be able, without special effort or advanced technical skills, to see, obtain, and use all electronically available information that is relevant to their health, care, and choices – of plans, providers, and special treatment options." The types of information envisioned are both specifically about the individual (which requires protection of the individual's privacy) and information of general interest that should be widely available (e.g., a health plan's provider network, formulary, and coverage policies). The agency contrasts the difficulties that patients can experience in obtaining access to their electronic health information through multiple provider and plan portals or applications with the ease with which consumers can choose a navigation application to choose a route.

An API is described as a set of commands, functions, protocols, or tools published by a software developer that enables other developers to create programs (applications or "apps") that interact with the software without needing to know its internal workings and that maintain consumer data privacy standards.

By using its authority in Medicare, Medicaid, CHIP and over QHPs in FFEs to require that plans in these programs adopt and implement openly published APIs ("open APIs"), CMS intends that enrollees in these plans will be able to use an application of their choice to access their own electronic health information and other information to manage their health. CMS clarifies that an open API does not mean that applications and application developers would have unfettered access to personal or sensitive information about individuals. It means that the open published technical and other information specifies what a developer needs to know to connect to and obtain the data available through the API.

As described further below, CMS is relying on the API technical standard proposed in the separately published ONC proposed rule on interoperability (summarized in Appendix A). However, CMS emphasizes that it is not proposing to require health plan issuers to use ONC-certified Health IT Modules to make administrative data such as claims history or provider directory information available to enrollees.

CMS sees three key attributes of open APIs: standardized API technologies, technically transparent APIs, and APIs implemented in a pro-competitive manner.

With respect to transparency, CMS says that information material to API users (those that use or create software applications that interact with the API) includes all terms and conditions for use of the API, including terms of service, restrictions, limitations, obligations, registration processes, or other similar requirements needed to:

- Develop software applications to interact with the API;
- Connect software applications to the API to access electronic health information through the API;
- Use any electronic health information obtained by means of the API technology; and
- Register software applications to interact with the API.

On the issue of pro-competitive APIs, CMS reiterates that individuals should be able to choose and use an application to connect and access, without special effort, their electronic health information held by health care providers, health plans, or any health information networks, *within practical and prudent limits* that do not needlessly hinder their ability to connect to the API in a persistent manner. It says that acceptable limits in this context include technical compatibility and ensuring that the application does not impost an "unacceptable level of risk to a system" when connecting to an API, consistent with HIPAA Privacy and Security Rules. CMS recognizes the need for organizations subject to the open API proposal need to take reasonable steps to fulfill duties under HIPAA (45 CFR 160.103) and all applicable privacy and security rules. However, this should not be an opportunity to engage in anti-competitive practices.

- An example of pro-competitive practices is advising enrollees that they are not limited to using the organization's own or preferred applications and providing information about how the enrollees can request their health information through a third-party API of their choosing.
- An example of an anti-competitive practice is refusing to assess the technical compatibility or security risk of an application provided to prospective enrollees by a competing plan.

CMS acknowledges receiving many comments in the past raising concerns about the privacy and security risks created by an API connecting to third-party applications, and it understands that HIPAA-covered entities and business associates are responsible for protected health information (PHI). However, CMS notes that some stakeholders might believe they are responsible for determining whether an application to which an individual directs their PHI applies appropriate safeguards for the information it receives. It says that that based on Office of Civil Rights (OCR) guidance, covered entities are not responsible under HIPAA rules for the security of PHI once it has been received by a third-party application chosen by an individual. A variety of OCR

guidances are cited, in particular HIPAA FAQ 2060[1] in which OCR says that "…individuals have the right under HIPAA to have copies of their PHI transferred or transmitted to them in the manner they request, even if the requested mode of transfer or transmission is unsecure, as long as the PHI is "readily producible" in the manner requested, based on the capabilities of the covered entity and transmission or transfer in such a manner would not present an unacceptable level of security risk to the PHI on the covered entity's systems, such as risks that may be presented by connecting an outside system, application, or device directly to a covered entity's systems (as opposed to security risks to PHI once it has left the systems)."

With respect to stakeholder concerns that unscrupulous actors could use direct-to-consumer applications to profit from obtaining and using or disclosing PHI without the individual's authorization, CMS notes that the Federal Trade Commission has the authority to investigate and take action against unfair trade practices. In order to ensure that enrollees are better informed about how to protect their PHI, in section III CMS proposes requirements on payers to assist in this regard.

CMS also notes that not all enrollee requests for information would be readily transferable through an API, and that the responsibility of covered entities to provide this information or all information through other means is not limited as a result of the proposed rule's API requirements.

The proposed specific standards for APIs discussed in section III.C include content and vocabulary standards for representing electronic health information and technical standards by which an API must make electronic health information available. The proposed standards would align with the interoperability standards in the ONC proposed rule. In doing this CMS says that it intends to prevent regulated entities form implementing API technology using alternative technical standards such as proprietary standards or others that are not widely used to exchange electronic health information in the U.S. Use of earlier versions of the technical standard would also be precluded.

Exceptions are proposed under which other content and vocabulary stands could be used. These are 1) where other such standards are expressly mandated by law, and 2) where no standard exists within 45 CFR part 162, 42 CFR 423.160 or the ONC proposed 45 CFR 170.213 and 170.215.

CMS welcomes comments on its proposal to align the standards in this proposed rule with those in the ONC proposed rule, as well as the best method to provide support in identifying and implementing the applicable content and vocabulary standards for a particular data element. **In addition, public comments are sought on an alternative under which CMS would separately adopt the proposed ONC standards identified throughout this proposed rule, as well as future standards on interoperability, content and vocabulary.** CMS expects that this alternative would incorporate by reference the technical standards and the content and vocabulary standards into CMS regulations, replacing references to the ONC regulations. **CMS specifically seeks comment on whether this alternative would risk misalignment of standards or versions of standards across HHS programs and asks about the benefits or**

[1] https://www.hhs.gov/hipaa/for-professionals/faq/2060/do-individuals-have-the-right-under-hipaa-to-have/index.html

burdens of separately adopting standards for each program. It wants to know how this option might impact health IT development timelines, how misalignment of standards might impact system implementation, and other factors related to the technical implementation of the requirements.

B. Content and Vocabulary Standards

The specific content and vocabulary standards proposed in this rule are:

- USCDI Version 1[2], as proposed in the ONC proposed rule (45 CFR 170.213), where these are the only available standards for the data type or element;
- HIPAA Administrative Simplification transaction standards (45 CFR part 162) or the Medicare Part D e-prescribing transaction standards (42 CFR 423.160) where required by law or when these are the only standards available for the data type or element; or
- When a specific data type or element might be encoded or formatted under different standards (45 CFR part 162 or 42 CFR 423.160 or the proposed 45 CFR 170.213), any of these may be used as appropriate.

The USCDI Version 1 data set establishes a minimum set of data classes that would be required to be interoperable nationwide. It is designed to be expanded in an iterative and predictable way over time. As proposed by ONC for HHS adoption at 45 CFR 170.213, it also includes the standards referenced by certification criteria adopted in 45 CFR part 170, to which health IT, such as Health IT Modules presented for certification under ONC's Health IT Certification Program, must conform. CMS believes that because application developers are already using these standards, their implementation for CMS programs should not add new burdens to the industry.

CMS clarifies that for purposes of formatting, making available, and sending electronic data under this proposed rule, it would require use of: (1) the content and vocabulary standards identified in 45 CFR part 162 regardless of whether the entities are covered entities, and (2) the part D e-prescribing standards in 42 CFR 423.160 to exchange e-prescribing and related data (such as drug formulary and preferred drug list data) regardless of whether they are conducting a part D e-prescribing transaction. Further, CMS notes that in requiring the use of these standards the existing regulations at 45 CFR part 162 and 42 CFR 423.160 would not be altered.

Regarding information exchanges where multiple standards might apply, CMS gives payers the flexibility to choose any of the applicable standards while conforming to the API standards in the ONC proposed rule. It expects that payers will use the standards that are most efficient and effective based on their systems, data mapping considerations or standards that best meet the needs of enrollees.

Regarding data for which no standard is adopted under the referenced regulations, CMS encourages payers to implement additional, widely used, consensus-based standards identified by other means (e.g., by HHS for other purposes or through a consensus standards development organization), while maintaining compatibility with the API technical standards. Pilot testing of emerging standards is also encouraged, but CMS notes that payers that choose to make non-standardized data available through their APIs would be required to ensure that their API

[2] The USCDI is detailed at https://www.healthit.gov/USCDI

documentation provides sufficient information to an application developer for their applications to handle this information accurately and automatically.

C. API Standard

CMS proposes to adopt by cross reference the proposed API technical standard included in the ONC proposed rule (45 CFR 170.215). By doing this, it is effectively proposing to require the use of the foundational Health Level 7 (HL7®) Fast Healthcare Interoperability Resources (FHIR) standard, several implementation specifications for FHIR, and complementary security and app registration protocols (OAuth 2.0 and OpenID Connect Core).

CMS notes the industry's rapid embrace of the FHIR standard, which enables users to access health care resources over the internet via a standardized RESTful[3] API, and it notes that with one exception the API technology standards are consensus standards that are preferred for use in government programs under the National Transfer &Advancement Act of 1995 and OMB Circular A-119.

CMS does not anticipate that all of the standards, implementation specifications, and protocols proposed in the ONC rule at 45 CFR 170.215 would be directly relevant to every use. For example, authenticating end users' identities may not be needed when the information requested and released to an application through the API is not PHI, but widely available information such as the provider directory. In addition, CMS notes that "an API implemented by regulated entities described in section III.C of this proposed rule is not required to be certified by ONC under the ONC Health IT Certification Program. Because the data required by payers that would be regulated under this proposed rule would extend beyond the USCDI Version 1 data set, ONC certification would not be sufficient to ensure that an API would support the full range of required data elements required [as described in section III.C below]."

Recognizing that work will need to be done by health IT developers and their customers to comply with the ONC proposed rule and this proposed rule, HHS expects to provide organizations subject to this proposed rule with technical assistance and guidance that incorporates industry feedback. Readers are encouraged to read the ONC proposed rule and also resources on the HL7 FHIR standard (https://www.hl7.org/fhir/overview.html and the USCDI version 1 standard.

Finally, CMS hopes to see further innovation and advancement in standards. As an example, it offers that the proposed rule does not include a requirement that payers offer patients or providers the ability to write information to patient records via the API, but it hopes that organizations build toward that capacity as fast as possible.

D. Updates to Standards

CMS proposes that payers may use updated versions of required standards if the updated version is required by another applicable law or is not prohibited under another law, provided that (1) the Secretary has not prohibited their use, (2) the ONC has approved updates to its standards for use in the ONC Health IT Certification program, and (3) use of the updated version does not disrupt an end-users ability to access data through the API. CMS says that it will publish regulatory

[3] "RESTful" interfaces" are those that are consistent with Representational State Transfer (REST) architectural style and communications approaches to web services development.

guidance in cases where there are multiple updates of a single standard and HHS determines that only the latest update should be used.

Under this proposed flexibility, those entities required to implement an open API under this proposed rule could upgrade to newer versions of the required standards at any pace they wish, subject to the limiting conditions described above. However, they would also be required to continue to support connectivity, and make the same data available, for end users using applications that have been built to support only the adopted version(s) of the API standards.

CMS notes that the ONC expects to use an expanded section of the Interoperability Standards Advisory (ISA) web platform to facilitate public transparency and engagement and to annually publish the final list of National Coordinator-approved advanced versions that health IT developers could elect to use consistent with the Standards Version Advancement Process.

III. Patient Access Through APIs

A. Background on Medicare Blue Button

CMS describes the Medicare Blue Button 2.0 initiative, under which beneficiaries can access claims data for Medicare parts A, B and D and share the information through an API. CMS believes beneficiaries will benefit from having secure access to claims data in a standardized computable format. It further expects the Medicare Blue Button 2.0 will increase competition among technology innovators who will work to find better ways for beneficiaries and caregivers to use claims data to address health needs.

B. Expanding the Availability of Health Information

The benefits of information access are discussed. CMS views the combination of claims and encounter data used in conjunction with EHR data as providing a broader picture of an individual's interactions with the health care system than EHR data alone. It says these data can empower individuals to make informed health care decisions, and individuals can facilitate communication with multiple health care providers by allowing them to access the same information through an open API. CMS notes that the open API proposal would provide an additional method for individuals to exercise the HIPAA right of access to PHI, although it may be that not all information subject to the HIPAA right of access would be transferable through the API.

C. Open API Proposal for MA, Medicaid, CHIP, and QHP Issuers in FFEs

The specific requirements for payers to implement, test, and monitor the proposed openly-published API that is accessible to third-party applications and developers are detailed in this section of the proposed rule. "Nearly identical" regulatory language is proposed for each payer; the sections of 42 CFR that would be affected are for MA organizations (422.119); state Medicaid fee-for-service programs (431.60); Medicaid managed care plans (438.242(b)); CHIP fee-for-service programs (457.730); and CHIP managed care plans (457.1233(d)). In addition, 45 CFR 156.221 would be modified, which pertains to QHPs in FFEs. With respect to QHPs, the open API proposal would not apply to stand alone dental plans offered in FFEs.

The scope and volume of information proposed to be provided or made accessible through the API includes:

- adjudicated claims (including cost);
- encounters with capitated providers;
- provider remittances;
- enrollee cost-sharing;
- clinical data, including lab results where available;
- provider directory (not required of QHP issuers in FFEs); and
- formularies (not required of QHP issuers in FFEs).

CMS believes these proposals would support and modernize existing provisions that require MA plans, Medicaid managed care organizations, and CHIP managed care entities to provide basic information to enrollees on how to obtain plan benefits and to facilitate decision making about plan choice, providers and benefits. Although information about the provider directory and formularies is available online, CMS believes that integrating this information into the API would allow greater use by enrollees, allowing them to share information with providers, family, and caregivers.

Because consumers routinely perform daily tasks on mobile phones using secure applications, CMS believes that it should be possible to also obtain and use health information this way.

The proposed regulations for each payer follow the same structure. In each section, paragraph (a) would require the entity to implement and maintain an open API that permits third-party applications to retrieve, with the approval and direction of the individual, data specified in paragraph (b) through the use of common technologies and without special effort from the beneficiary. "Common technologies" refers to smart phones, home computers, laptops or tablets and the like. The term "without special effort" reflects CMS' expectation that third-party software as well as proprietary applications and web portals operated by the payer could be used to connect to the API and provide the enrollee access to the data. Paragraph (c) identifies the technical standards for the API; paragraph (d) the documentation requirements; paragraph (e) authority for the payer to deny or discontinue access to the API; paragraphs (f) and (g) requirements for posting information on security and privacy for beneficiaries. These requirements and others are described further below.

Statutory Authority to Require Implementation of an Open API. With respect to each payer, CMS describes the statutory authority under which it is proposing the open API requirements; that discussion is not detailed for purposes of this summary. While it does not have authority to apply the open API proposal to QHPs solely in state-based exchanges (SBEs), CMS encourages SBEs to consider whether a similar requirement should apply to QHPs in these exchanges.

API Technical Standard; Content and Vocabulary Standards. As discussed earlier, the payers covered by this proposed rule would be required to implement open API technology that conforms with the API technical standards proposed at 45 CFR 170.215 in the ONC proposed rule. In addition, the content and vocabulary standards at 45 CFR part 162 and 42 CFR 423.160 and in proposed 45 CFR 170.213 (described in section II.B above) would be required. In addition to the amendments to the regulatory sections listed above for each payer, conforming changes to

other regulatory text are proposed. As discussed in section II.D, CMS proposes payers may use updated versions of required standards under certain circumstances.

Data Required to be Available Through Open API; Timeframes for Data Availability. CMS proposes that, at a minimum, the information listed below be made available through the API. The specific data requirements vary for each payer (e.g., data on adjudicated part D drug claims is required for MA plans).

- adjudicated claims data, including provider remittances and beneficiary or enrollee cost- sharing data;
- encounters from capitated providers;
- clinical data, including laboratory results (but only if managed by the payer);
- provider directory information;
- formulary information (for MA-PD plans) or information about covered outpatient drugs and preferred drug lists (for state Medicaid and CHIP agencies, Medicaid managed care plans and CHIP managed care entities).

Adjudicated claims data would include data on approved and denied claims, and that for which the plan has made an initial payment decision even when the period during which an enrollee can file an appeal is still in effect, or when the enrollee has filed an appeal and is awaiting a reconsideration decision. **CMS specifically requests comments from plans regarding the feasibility of including such claims data, including any possible timing issues.**

The proposed time requirements within which the required information would have to be made available to the API vary by payer, as shown in the following table.

	MA	**Medicaid and CHIP**	**QHP in FFE**
Proposed regulatory text	42 CFR 422.119	42 CFR 431.60 and 457.730*	45 CFR 155.221
Claims data	1 business data after receipt	1 business day after processed	1 business day after processed
Encounter data	1 business data after receipt	1 business data after receipt*	1 business data after receipt
Provider directory	30 calendar days after changes	30 calendar days after changes	N/A
Clinical data	1 business data after receipt (if managed by the organization)	1 business data after receipt (if managed by the state)	1 business data after receipt (if managed by the issuer)
Formulary (or for Medicaid and CHIP FFS info on covered outpatient drugs)	Unspecified	1 business day after updates effective	N/A
*Same requirements would be applied by reference to Medicaid and CHIP managed care plans at 438.242 and 457.1233			

CMS notes that to the extent that providers delay in submitting encounter data to payers, this will delay the availability of that information from the payer to the patient through the API. It recommends that payers consider whether contracts with network providers should include timing requirements for the submission of encounter data and claims.

The clinical data requirement as proposed would effectively make any clinical data included in the USCDI (Version 1), proposed in the ONC proposed rule (45 CFR 170.213), available through the API if the data is received and maintained by the payer as part of its normal operations. **CMS seeks comment on any barriers that may discourage payers from obtaining, maintaining and sharing these data.**

With respect to drug benefit data (pharmacy and formulary data), CMS notes that MA-PD plans must already provide pharmacy directory information. In this rule CMS is not proposing a timeframe for making this information available (or updating it) through the API; **comments are sought specifically on whether to address timing in the regulatory text for MA-PD plans or otherwise impose a timeframe for making the information available through the API.**

Because under existing 45 CFR 156.230(c) QHPs in FFEs must make provider directory information accessible in machine-readable format, CMS does not believe the benefits of making it available through the API outweighs the burdens on QHP issuers. For the same reason, the proposed requirement to provide preferred drug list information would not be applied to QHPs in FFEs.

Documentation Requirements for APIs. Under the proposed rule, regulated payers would be required to publish complete documentation regarding the API on their website or via a publicly accessible hyperlink. CMS expects that any person using the internet could access the information without any preconditions or additional steps beyond downloading and using a third-party application to access data through the API. By "additional steps" CMS means to preclude actions such as collecting a fee to access the documentation, requiring the reader to receive a copy via email, or requiring the user to read promotional material or agree to receive future communications from the organization making the documentation available. The publicly accessible documentation would be required to include, at a minimum, the following:

- API syntax, function names, required and optional parameters supported and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns.
- The software components and configurations an application must use in order to successfully interact with the API (for example, to connect and receive data through the API) and process its response(s).
- All applicable technical requirements and attributes necessary for an application to be registered with any authorization server(s) deployed in conjunction with the API.

CMS notes that similar requirements are proposed in the ONC proposed rule API criteria for developers and users of health IT but is proposed here to apply specifically to the API technology used by payers subject to this proposed rule.

Routine Testing and Monitoring of Open APIs. CMS proposes that the API be routinely tested and monitored to ensure it is functioning properly, including assessments to verify that the API is

fully and successfully implementing the HIPAA privacy and security requirements (45 CFR part 164, 42 CFR parts 2 and 3) and other such federal, state, tribal or local laws that apply to the entity. In the testing payers would assess the API's authentication features to verify the identity of individuals to ensure that enrollees (or designated representatives) can only access PHI that belongs to them.

Compliance with Existing Privacy and Security Requirements. **CMS requests comments on whether existing privacy and security standards,** including those under HIPAA, are sufficient for these proposals or whether additional privacy and security standards should be required by CMS.

Issues Related to Denial or Discontinuation of Access to the API. Under OCR guidance, when an individual requests to receive their data under the HIPAA Right of Access, covered entities must comply, including having to transmit data to a third party. As OCR guidance has noted, disagreement with the requesting individual about the worthiness of the third-party recipient of PHI or concerns about what that third party might do with PHI are not grounds for denying a request. However, a covered entity is not expected to tolerate unacceptable risk to its own systems as determined by its own risk analysis. Therefore, it may be appropriate for a payer covered under the proposed rule to deny or terminate specific applications from connecting to its API if the risk posed to the PHI on its systems is unacceptable or if the application violates the terms of use of the API technology.

The proposed regulations specify the circumstances under which the regulated payers, which are all HIPAA-covered entities, may decline to establish or may terminate a third-party application's connection to their API while remaining in compliance with the proposed open API requirements. CMS notes that the circumstances apply to specific applications and not the third party itself. For instance, if an individual requests that a HIPAA covered entity provide the individual's information through other means (i.e., not through an API) to a third party that has been denied access through the API, the covered entity would be required to approach the request as if the application's API request or connection had not occurred.

Specifically, CMS proposes that a payer that would be regulated by this proposed rule could deny or discontinue any third-party application's connection to the open API if it:

- Reasonably determines that allowing an application to connect or remain connected to the API would present an unacceptable level of risk to the security of protected health information on the organization's systems; and
- Makes this determination using objective, verifiable criteria that are applied fairly and consistently across all applications and developers through which enrollees seek to access their electronic health information, including criteria that may rely on automated monitoring and risk mitigation tools.

CMS notes that criteria and tolerable risk levels appropriate to assessing risk to an API for providing access to publicly available information such as provider directories, may differ from those involving requests regarding non-published PHI. Further, CMS anticipates that where a third party's connection to an API has been terminated, it might be feasible for the organization to allow it to re-connect if the underlying problem and risk to the API has been addressed.

Enrollee and Beneficiary Resources Regarding Privacy and Security. Effective January 1, 2020, payers that would be regulated by this proposed rule would be required to make available to current and former enrollees certain information related to privacy and security of PHI. Each payer would be required to provide educational resources on its website and through other normal communication channels with current and former enrollees seeking to access their health information held by the payer. This could include customer portals, online customer service, and other locations.

At a minimum the resources would have to explain in non-technical, simple and easy-to-understand language:

- General information on steps the individual may consider taking to help protect the privacy and security of their health information, including factors to consider in selecting an application, and understanding the security and privacy practices of any application to which they will entrust their health information; and
- An overview of which types of organizations or individuals are and are not likely to be HIPAA covered entities, the oversight responsibilities of OCR and FTC, and how to submit a complaint to OCR and FTC.

CMS believes that organizations could meet this requirement by using materials available on the HHS or FTC websites that are designed for consumer audiences. An organization choosing to use its own materials would be responsible for ensuring the information remains current if laws and policies change over time. **CMS seeks comment on what specific additional information resources would be most useful to entities in meeting this requirement.** Comments received will be used to prioritize HHS work on developing informational resources as well as making a decision for the final rule.

Exception or Provisions Specific to Certain Programs or Sub-Programs. CMS reviews provisions in the proposed rule that are unique to certain types of plans. Specifically, the exclusion of stand-alone dental plans from the requirements proposed for QHPs in FFEs as described earlier, and the provisions specific to Part D (e.g., accessibility of Part D claims data) that would apply to MA-PD plans and not to other MA plans.

In addition, CMS proposes that an FFE may grant exceptions from the open API requirements for plans applying for QHP certification if the FFE determines it is in the best interests of the qualified individuals and employers where it operates. To receive an exception a plan applying for QHP certification would have to provide a narrative justification describing the reasons why it cannot reasonably satisfy the requirements, the impact of non-compliance upon enrollees, the current or proposed means of providing health information to enrollees, and solutions and a timeline to achieve compliance. CMS expects that these exceptions would be provided in limited circumstances such as small issuers, issuers who are only in the individual or small group market, financially vulnerable issuers, or new market entrants demonstrating that implementing an open API would be a barrier to their ability to provide coverage to consumers and where not certifying the QHP would limit plan options for consumers. **CMS seeks comment on other circumstances in which an FFE should consider providing an exception.**

Applicability/Effective Dates. Proposed effective dates of the open API requirements vary by payer.

- MA organizations with contracts to offer any MA plan would be required to comply with the API requirements beginning on January 1, 2020 or later. **CMS seeks feedback from the industry on this date, and requests comment from MA organizations abouttheir capability to implement an API consistent with the proposed rule and the costs associated with compliance by January 1, 2020 compared with a later date.**
- For Medicaid and CHIP agencies operating FFS programs and Medicaid and CHIP managed care organizations, the open API requirements would be effective beginning July 1, 2020, regardless of when any managed care contract started. **CMS solicits comment on whether additional flexibility would be needed to take into account** the contract terms that states use for managed care plans.
- For QHP issuers in FFEs, the API requirements would be effective for plan years beginning on or after January 1, 2020. **CMS seeks comment on how long issuers, particularly smaller issuers, anticipate it would take to come into compliancewith the requirements.**

Information Sharing Between Payers and Providers through APIs: Request for Information. CMS anticipates that in the future payers and providers may seek to coordinate care and share information on an overlapping patient population in a single transaction. This could facilitate better understanding of where patients are receiving care to better manage their care. While in some places regional health information exchange might coordinate such transmissions, direct provider-to provider or plan-to-plan exchange through existing trusted networks of beneficiary- facing third-party applications might be more appropriate elsewhere.

For possible consideration in future rulemaking CMS seeks comment on the feasibility of provider to request a download on a shared patient population, and whether this would leverage open APIs. Comments are sought on requirements for patient notice and consent, and applicable legal and regulatory requirements, and whether the data transfer could be cumulative over time and between various providers. CMS further seeks input on the usefulness to providers of obtaining all their patients' utilization history in a timely and comprehensive fashion. Input is also sought on potential unintended consequences that could result from allowing a provider to access or download information about a shared patient population through an open API. Finally, comments are sought on the associated burden on plans to exchange these data as well as identification of potential statutory or regulatory barriers to such data exchange.

D. Impact Analysis

In the collection of information requirements section of the proposed rule, CMS estimates that affected payers would bear an aggregate one-time cost of $275 million to implement the proposed API requirements ($789,356 per organization or state). In addition, estimated annual aggregate costs total an estimated $55 million for activities such as testing, upgrades andvetting of third-party applications ($158,360 per organization or state).

IV. API Access to Published Provider Directory Data

This section of the proposed rule further describes the proposal to make provider directory information broadly available through the API, which may differ from proposals related to accessibility of patient-specific data. Current regulations require the payers that would be regulated under this proposed rule to make the provider directory available on a website or in the

case of QHPs in FFEs, publicly accessible in addition to distribution and access for enrollees. However, CMS says that making the information available through an API could support development of applications that would pull in current information about available providers to meet the needs of enrollees. For example, a referring provider could use the up-to-date contact information obtained from the API directory to securely send patient information to the receiving provider. CMS believes provider burden would be reduced also by allowing payers to share more widely the information about providers in their network and whether or not they are accepting new patients.

Under the proposed rule, payers would make standardized information about their provider networks available through API technology, so that third party software could access and publish the information. The information would be for current enrollees, prospective enrollees, and possibly the general public depending on existing regulations. The API technology would need to conform to the API standards proposed in the ONC proposed rule (45 CFR 170.215). As noted earlier, CMS does not propose that QHPs in FFEs be subject to this requirement because current regulations require them to make the information available in machine-readable format. **CMS seeks comment on whether the proposed requirement for access to provider directories through the API should also apply to QHP issuers, or whether this would be overly burdensome on them.**

CMS notes that the provider directory information made available through the API would be as accessible as it is required to be when posted on a website. The security protocols proposed at 45 CFR 170.215 that are specific to authenticating users and confirming individuals' authorization or request to disclose their personal information would not apply in the case of public access to provider directory information through APIs. Steps an organization needs to take to mitigate the potential security risks of allowing any application to connect to its API should be appropriate to the level of risk associated with accessing otherwise public information through API technology.

As mentioned earlier, CMS intends to develop additional guidance, incorporating feedback from industry that provides implementation best practices relevant to FHIR-conformant open APIs to help organizations subject to the requirements proposed in this rulemaking. **CMS seeks comment on what specific resources would be most helpful to organizations implementing APIs under requirements proposed in this proposed rule.**

V. Health Information Exchange and Care Coordination Across Payers: Establishing a Coordination of Care Transaction to Communication Between Plans

CMS proposes that the payers regulated under this proposed rule must maintain a process for the electronic exchange of the data classes and elements included in the UCSDI Version 1 data set standard proposed in the ONC proposed rule (45 CFR 170.213) and described in section II.B above. This information when received from another payer would be required to be incorporated into the receiving payer's records about the enrollee. At the request of a current enrollee, the payer must receive the data from any other health plan that has provided coverage to the enrollee within the preceding 5 years; for up to 5 years after disenrollment send data to any other plan that currently covers the enrollee; and for a period of up to 5 years after disenrollment send data to a recipient designated by a current enrollee. This requirement would be effective starting January 1, 2020. **Comments are specifically requested on the effective date.**

CMS believes that the proposed use of the USCDI to exchange information furthers care coordination. Examples offered are reducing the need for health care providers to write letters of medical necessity; reducing instances of inappropriate step therapy; reducing repeated utilization reviews, risk screenings and assessments; streamlining prior authorization processes; and reducing instances where health care provider needs to intervene with a plan to ensure a patient receives needed treatment. These are all areas which CMS says stakeholders have previously raised as examples of administrative burdens.

In addition, by providing access to multiple years of their health care information, CMS believes the proposal would provide patients with a more comprehensive history of their medical care. The UCSDI data set includes laboratory and other test results, medications, health concerns, clinical notes, assessments and treatment plans and other data points needed for care coordination. **CMS seeks comment on how plans might combine records and address error reconciliation or other factors in establishing a longitudinal record for each patient.**

This proposal would allow for multiple methods for electronic exchange of information, not limited to the open API as proposed in this rule. CMS considered requiring the use of the API for this purpose but decided that regional health information exchange, where available, could serve this purpose. **CMS seeks comment on whether to require the use of the API for exchange of UCDSI data.** CMS expects enrollees to be able to request an exchange of the USCDI data set at any time, not just at enrollment or disenrollment. **Comments are sought on other means that the applicable plans may prefer to use for meeting this requirement and whether CMS might be able to leverage its program authority to facilitate the data exchanges contemplated by this proposal.** Further, **comments are sought on how to support patients and providers in situations where a plan subject to this proposed requirement may be exchanging patient health information with other plans that are not similarly required to exchange USCDI data sets for enrollees.**

With respect to the proposal that a patient would be allowed to request information from a prior plan for up to 5 years after disenrollment, CMS notes that this is considerably less than current data retention policies. Under existing regulations MA plans, Medicaid and CHIP managed care plans, and QHPs in FFEs must retain records for 10 years.

In the regulatory impact analysis section of the proposed rule, CMS estimates that this proposal would have minimal costs on plans. It says it is difficult to quantity the impact because the methods that plans will use to share information (e.g., APIs, exchanges) cannot be predicted.

CMS considered proposing that plans be required to exchange all the data that would be available through the API under this proposed rule (as summarized in section III.C) but chose to limit this requirement to the USCDI data set due to challenges of ingesting data and reconciling errors. **Comments are sought on whether the USCDI data set is comprehensive enough to facilitate the type of care coordination and patient access envisioned in the proposed rule, or whether additional data fields from the API requirement should also be required under this provision.**

Dual eligible enrollees who are enrolled in both an MA plan and a Medicaid managed care plan would be supported under this proposal, CMS believes, because both plans would be subject to the USCDI data exchange requirement. **CMS seeks comment on how plans should coordinate**

care and exchange information in these situations; on the associated burden on plans under the proposal, and on potential legal barriers to exchange the USCDI data set. It asks whether there are federal, state, local and tribal laws governing privacy for specific use cases (e.g., the care of minors for certain behavioral health treatments) that raise additional considerations that CMS should address in the final rule or in guidance.

Finally, **comments are sought on CMS' assumption that the proposed data exchange of USCDI data among plans regulated under this proposed rule may qualify as a quality improvement activity for purposes of the medical loss ratio requirements** with respect to QHPs in FFEs and similar standards for MA plans and Medicaid managed care plans, and the related implications.

VI. Care Coordination Through Trusted Exchange Networks: Trusted Exchange Network Requirements for MA Plans, Medicaid Managed Care Plans, CHIP Managed Care Entities, and QHPs in the FFEs

CMS proposes that the payers that would be regulated under this proposed rule must participate in trusted exchange networks in order to improve interoperability. It believes that these networks allow for broader interoperability beyond one health system or point-to-point connections among payers, patients and providers. CMS notes that trusted exchange networks are gaining momentum and participants include several federal agencies, EHR vendors, retail pharmacy chains, large provider associations and others. With widespread payer participation, CMS believes that these frameworks might allow for more complete access and exchange of all electronically accessible health information, which would lead to better use of the data.

Specifically, CMS proposes that beginning January 1, 2020, MA plans, Medicaid and HIP managed care plans, and QHPs in FFEs must participate in a trusted exchange network which:

> (i) Is capable of exchanging PHI, (defined at 45 CFR 160.103) in compliance with all applicable state and federal laws across jurisdictions;
>
> (ii) Is capable of connecting to inpatient electronic health records and ambulatory electronic health records; and
>
> (iii) Supports secure messaging or electronic querying by and between providers, payers and patients.

In the regulatory impact analysis section of the proposed rule, CMS states its view that this proposal would impose minimal additional costs on plans.

In January 2018 ONC released the draft Trusted Exchange Framework for public comment; **comments are sought here on how the proposed requirements might be aligned in the future with section 4003(b) of the Cures Act, and on how the proposed effective date of January 2020 and on the benefits and challenge affected payers may face in meeting this requirement, for consideration in future rulemaking.** Additionally, **comments are sought on CMS' assumption that the proposal to require participation in a trusted exchange network may qualify as a quality improvement activity for purposes of the medical loss ratio requirements** with respect to QHPs in FFEs and similar standards for MA plans and Medicaid managed care plans, and the related implications.

VII. Improving the Medicare-Medicaid Dually Eligible Experience by Increasing the Frequency of Federal-State Data Exchanges

CMS proposes to increase the frequency of federal-state data exchanges for individuals dually eligible for Medicare and Medicaid. It believes that the interoperability of CMS eligibility systems is critical to modernizing the programs and improving the experiences of beneficiaries and providers, and sees increasing the frequency of data exchanges as a strong first step.

A. State Buy-in for Medicare Parts A and B

Currently, all states and the District of Columbia have agreements with CMS to facilitate state "buy-in" of the Medicare Part B premium on behalf of dual eligibles; 36 states and DC have a buy-in agreement for part A premiums. Data is submitted by the state via an electronic file transfer (EFT) exchange setup; CMS responds and may push updates from the Social Security Administration such as a change in the beneficiary identification number or address.

Current regulations are silent on frequency of data exchange, but guidance provides that states should exchange buy-in data at least monthly, with the option for daily or weekly exchange. States may also choose how frequently to receive the CMS response data file. CMS reports that 31 states and DC are submitting buy-in data to CMS daily and 28 states and DC are receiving response files from CMS daily. CMS is concerned that in states that exchange data monthly the lag in updating buy-in data means that the state or beneficiary may be paying premiums for longer than appropriate. Recoupment and redistribution of funds is a burdensome administrative process between the beneficiary, state, CMS, and SSA. It can take multiple months to correct and resubmit an improperly processed transaction, exacerbating the delays in appropriately assigning premium liability.

Therefore, CMS proposes to modify existing regulations to require that all states participate in daily exchange of buy-in data to CMS (meaning every business day for which a new transaction is available to transmit). The change would be effective April 1, 2022; CMS believes this will provide the affected states (19 for submitting buy-in data and 22 for receiving it) with sufficient time to phase in operational changes or bundle this requirement with other systems updates. CMS believes the one-time cost to a state would be a little less than $80,000 per change (i.e., $160,000 for a state that needs to change make changes for both sending and receiving data daily). In the regulatory impact analysis section of the proposed rule, CMS estimates the aggregate cost to states of implementing this requirement would be $3.2 million.

B. Exchange of MMA Data Files

Under the Medicare Modernization Act (MMA) (P.L. 108-173) primary responsibility for prescription drug coverage for full-benefit dual eligibles shifted to the Medicare program. Implementing regulations (42 CFR 423.910) require states to report at least monthly a file identifying full-benefit and partial-benefit dually eligible beneficiaries in the state. This has come to be called the "MMA file" or "State Phasedown File." In addition to information exchange related to Part D, these data are used to support risk adjustment of MA plans, and to inform Part A and B eligibility and claim processing systems so that providers, suppliers and beneficiaries have accurate information on beneficiary cost-sharing obligations.

Most states submit the MMA data files at least weekly; only 13 states do so daily. Because dual eligibility status can change at any time, CMS believes that monthly status updates prevent access to the correct level of benefit at the correct level of payment. While it has instituted work-arounds, CMS believes more frequent data exchange would be preferred. Advantages of daily data exchange that CMS sees include enabling an earlier transition to Medicare coverage for prescription drugs; reducing claims paid erroneously by the state; effectuating an earlier shift to Medicare as primary payer for many services; aiding timely error identification and resolution; supporting states that promote enrollment in integrated care such as Dual-eligible Special Needs Plans, Medicare-Medicaid Plans, and the Programs for All-inclusive Care for the Elderly (PACE) by expediting the enrollment into Medicare; supporting earlier beneficiary access to Medicare Part D benefits and related subsidies sooner; and promoting protections for qualified Medicare beneficiaries (QMBs) by improving the accuracy of data for providers and QMBs on zero cost-sharing liability for services under Medicare Parts A and B.

Therefore, CMS proposes to update the frequency requirements (in 42 CFR 423.910(d) and conforming changes) to require that starting April 1, 2022, all states submit the required MMA file data to CMS daily (every business day for which a new transaction is available to transmit). CMS believes this effective date will provide states with enough time to make operational changes or bundle this required change with any new systems implementation. CMS estimates a one-time cost for a state to be a little less than $80,000 for this MMA data systems change. In the collection of information requirements section of the proposed rule CMS estimates the aggregate cost of this proposal to be $3 million.

C. Request for Comment

CMS seeks public comment for consideration in future rulemaking on how it can achieve greater interoperability of federal-state data for dually eligible beneficiaries, including in the areas of program integrity and care coordination, coordination of benefits and crossover claims, beneficiary eligibility and enrollment, and their underlying data infrastructure. Specifically, comments are sought on:

- Whether existing regulations, as well as those proposed in this rule, sufficiently support interoperability among those serving dually eligible beneficiaries, and if not, what additional steps would advance interoperability.
- How to enhance the interoperability of existing CMS processes to share Medicare data with states for care coordination and program integrity. How to improve the CMS and state data infrastructure to support interoperability (for example, more frequent data exchanges, common data environment, etc.). For eligibility, how interoperability can provide timely, integrated eligibility and enrollment status across Medicare, Medicaid, and related agencies (for example, SSA), and reduce the need for persons to provide, and states to collect/process, the same demographic information (for example, address, income).
- For provider enrollment in both Medicaid and Medicare, how interoperability can streamline provider enrollment and reduce provider and state burden to increase systems accuracy and beneficiary utilization of provider enrollment data (for example, disability competence, hours of service, types of insurance accepted, etc.).

- For coordination of benefits, including crossover claims, the underlying changes that would need to be made to support interoperability (for example, coding, file formats, provider/beneficiary identifier, and encounter versus FFS data).

Commenters are asked to include specific examples when possible while avoiding the transmission of protected information. A point of contact who can provide additional information upon request is also requested.

VIII. Information Blocking Background and Public Reporting

CMS reviews activities regarding information blocking. In 2015 ONC issued the Information Blocking Congressional Report, which concluded that information blocking is a serious problem and that the Congress should prohibit it and provide penalties and enforcement mechanisms to deter these practices. At the same time, the Congress enacted the Medicare Access and CHIP Reauthorization Act (MACRA), which requires that for purposes of demonstrating meaningful use of CEHRT, an eligible professional must demonstrate that he or she has not knowingly and willfully taken action (such as to disable functionality) to limit or restrict the compatibility or interoperability of CEHRT. MACRA imposed similar requirements on hospitals and critical access hospitals (CAHs). To implement these information blocking prevention provisions, CMS adopted attestation requirements, consisting of three statements about a provider's use of CEHRT[4]. To satisfy the Promoting Interoperability performance category of the Quality Payment Program (QPP) or, in the case of hospitals and CAHs, to meet the requirements of the Promoting Interoperability Program, a provider must attest "yes" to each of the statements.

A recent survey of health information organizations is cited, which found that half reported that EHR developers routinely engage in information blocking, and that one quarter reported that hospitals and health systems routinely do so.[5] Strengthening competitive position is seen as a motivation, but CMS says other research finds that these practices limit patient mobility, encourage consolidation and create barriers to entry for innovation.

The Cures Act added an information blocking provision (section 3022) to the PHS Act. It defines information blocking and creates possible penalties and disincentives to these practices. It

[4] The attestation requirement at 42 CFR 1375(b)(3)(ii) follows: *Support for health information exchange and the prevention of information blocking.* The MIPS eligible clinician must attest to CMS that he or she—(A) Did not knowingly and willfully take action (such as to disable functionality) to limit or restrict the compatibility or interoperability of certified EHR technology. (B) Implemented technologies, standards, policies, practices, and agreements reasonably calculated to ensure, to the greatest extent practicable and permitted by law, that the certified EHR technology was, at all relevant times—(*1*) Connected in accordance with applicable law; (*2*) Compliant with all standards applicable to the exchange of information, including the standards, implementation specifications, and certification criteria adopted at 45 CFR part 170; (*3*) Implemented in a manner that allowed for timely access by patients to their electronic health information; and (*4*) Implemented in a manner that allowed for the timely, secure, and trusted bi-directional exchange of structured electronic health information with other health care providers (as defined by 42 U.S.C. 300jj(3)), including unaffiliated providers, and with disparate certified EHR technology and health IT vendors. (C) Responded in good faith and in a timely manner to requests to retrieve or exchange electronic health information, including from patients, health care providers (as defined by 42 U.S.C. 300jj(3)), and other persons, regardless of the requestor's affiliation or technology vendor. Parallel language for hospitals and CAHs appears at 42 CFR 495.40(b)(2)(i)(I)(1) through (3).

[5] Julia Adler-Milstein and Eric Pfeifer, Information Blocking: Is It Occurring And What Policy Strategies Can Address It?, 95 Milbank Quarterly 117, 124–25 (Mar. 2017), available at http://onlinelibrary.wiley.com/doi/10.1111/1468-0009.12247/full

requires the Secretary to identify through rulemaking reasonable and necessary activities that do not constitute information blocking. The ONC proposed rule includes proposals to implement this requirement, and these are summarized in Appendix B to this summary.

In this rule, CMS proposes to publicly report information on eligible clinicians' attestations under the QPP on the Physician Compare website, and to report similar information on attestations of hospitals and CAHs under the Medicare Promoting Interoperability Program on a CMS public website. In the 2018 QPP final rule (85 FR 53827) CMS adopted a policy to include an indicator (as technically feasible) for any eligible clinician or group who successfully meets the Promoting Interoperability performance category and to include additional information on profile pages or in the downloadable data base on objectives, measures and activities with respect to this performance category.

Specifically, under this proposed rule an indicator would be added on Physician Compare for eligible clinicians and groups that submit a "no" response to any of the three attestation statements. If a "no" response is submitted the attestations would be considered incomplete and no indicator would appear. The indicator would be posted on the profile pages or the downloadable data base as feasible and appropriate, beginning with the 2019 performance period data available in late 2020. All public reported data are available for review and correction under the QPP targeted review process. CMS intends to determine the best display and wording after testing and sharing with stakeholders through the Physician Compare Initiative page and other communication channels. It reiterates that the proposal depends on the technical feasibility of using these data for public reporting.

Similarly, CMS would post information on a public website indicating any hospitals and CAHs that submit a "no" response to any of the three attestation statements. Information that is left blank would be considered incomplete and no information would be posted. The information would be posted beginning with the 2019 reporting period in late 2020. Hospitals and CAHs would have a 30-day preview period to review this information before it is publicly posted. During that time CMS would consider making changes on a case-by-case basis. Additional information would be provided outside the rulemaking process through usual communication channels.

IX. Provider Digital Contact Information

The Cures Act (section 4003) requires the Secretary to create a provider digital contact information index. To meet this requirement CMS has updated the National Plan and Provider Enumeration System (NPPES) to capture digital contact information for individuals and facilities. The NPPES supplies National Provider Identifier numbers to providers, maintains the NPI record and makes the information available online.[6] Since June 2018 the NPPEs has been updated to capture one or more pieces of digital contact information. This includes a Direct address and the ability to capture other endpoints for secure information exchange such as a FHIR server URL or query endpoint associated with a health information exchange. Each provider can maintain unique information or associated themselves with information shared

[6] See https://nppes.cms.hhs.gov/.

among a group of providers. NPPES has also added a public API which can be used to obtain contact information stored in the database.

Because many providers have not yet submitted digital contact information and what is there is frequently out of date, CMS proposes to public report the names and NPIs of providers who do not have digital contact information stored in the NPPES beginning in the second half of 2020.[7] **CMS seeks comment on the best way to pursue this public reporting initiative, including where the names should be posted, how frequently, and other information that would be helpful. Additional comments are sought on possible enforcement authorities to ensure that providers make digital contact information publicly available through the NPPES.** For example:

- Should Medicare reporting programs, such as MIPS, require eligible clinicians to update their NPPES data with their digital contact information?
- Should CMS require this information to be included as part of the Medicare enrollment and revalidation process?
- How can CMS work with states to promote adding information to the directory through state Medicaid programs and CHIP?
- Should CMS require providers to submit digital contact information as part of program integrity processes related to prior authorization and submission of medical record documentation?

CMS will review comments on these questions for possible consideration in future rulemaking.

X. Revisions to the Conditions of Participation for Hospitals and Critical Access Hospitals (CAHs)

CMS discusses the RFI on interoperability that it published in a number of proposed rules which requested input on how conditions of participation (CoPs) and similar CMS health and safety standards could be used to further advance electronic exchange of information. It notes that two previously proposed rules involving CoPs with provisions affecting interoperability are expected to be finalized this year. One involves discharge planning for hospitals, CAHs and home health agencies (80 FR 68126) and is expected by November 3, 2019. The other involves changes to CoPs for hospitals and CAHs to promote innovation, flexibility and improvement in patient care in hospitals and CAHs and is expected to be completed by June 15, 2019. CMS is committed to further steps to ensure that facilities that are electronically capturing information are also electronically exchanging it with other providers who have the capacity to accept it. It expects to require this through future rulemaking, with one option being alignment with TEFCA as described in section 4003 of the Cures Act.

In this rule, CMS proposes new CoPs for hospitals, psychiatric hospitals and CAHs that would require them to send electronic patient event notifications of a patient's admission, discharge and transfer to another facility or community provider. Patient event notifications are automated electronic communications from a discharging provider to another facility or to another

[7] CMS notes that under the 2015 Medicare and Medicaid HER Incentive Program Stage 3 final rule, a policy was finalized to collect a Direct address or other electronic service information in the NPPES, but this policy was not fully implemented due to limitations of the NPPES system at the time.

community provider identified by the patient. Virtually all EHR systems generate these messages using admission, discharge and transfer (ADT) messages.[8]

Under the proposal, the notification would include basic demographic information on the patient, the name of the sending institution and the diagnosis, unless prohibited by another applicable law. CMS encourages providers to offer more robust patient information and clinical data upon request in accordance with applicable laws.

For hospitals the proposed standard at a new paragraph (d) at 42 CFR 482.24 would apply only to hospitals that use an electronic medical records system with the capacity to generate information for patient event notifications. Hospitals with this capacity would be required to demonstrate that (1) the system's notification capacity is fully operational and that it operates in accordance with all state and federal laws and regulations regarding the exchange of patient health information; (2) the system uses the content exchange standard included in the proposed ONC regulations at 45 CFR 170.205(a)(4(i)) which is the HL7 CDA® R2 Implementation Guide: C-CDA Templates for Clinical Notes;[9] (3) the system sends notifications that must include the minimum patient health information (patient name, treating practitioner name, sending institution name, and, if not prohibited by other applicable law, patient diagnosis); (4) at the time of the patient's admission the system sends notifications directly or through an intermediary that facilitates exchange of health information to licensed and qualified practitioners, other patient care team members, and post-acute care services providers and suppliers that receive the notification for treatment, care coordination, or quality improvement purposes; have an established care relationship with the patient relevant to his or her care; and for whom the hospital has a reasonable certainty of receipt of notifications; and (5) either immediately prior to or at the time of the patient's discharge or transfer from the hospital, the system sends notifications directly or through an intermediary to licensed and qualified practitioners, other patient care team members, and post-acute care services providers and suppliers that meet the same conditions as in item (4).

CMS limits this proposal to hospitals that currently possess EHR systems with the capacity to general patient event notifications, recognizing that not all hospitals have been eligible for programs promoting adoption of EHR systems. While there is no specific ONC CEHRT standard for sending and sending electronic patient event notifications, CMS expects a hospital that has certified health IT for purposes of the Promoting Interoperability Program would have the basic capacity to general information for notification messages. CMS would not preclude hospitals from using other standards or features to support their notification systems. **Comments are sought on whether its proposal would achieve the goal of setting a baseline to generate information for electronic notifications, while still allowing for innovative approaches.**

CMS notes that while the requirement pertains to inpatients, it encourages hospitals to extend the notification systems to serve additional patients. For example, notification of a primary care physician when a patient has received care in the emergency room could help ensure the

[8] The current standard supporting these messages is available at http://www.hl7.org/implement/standards/product_brief.cfm?product_id=144 and the ONC Interoperability Standards Advisory at https://www.healthit.gov/isa/sending-a-notification-a-patients-admission-discharge-andor- transfer-status-other-providers.

[9] The regulatory reference changed from the pre-release version of this proposed rule. It was 170.299(f)(2).

appropriate follow-up care. **CMS seeks comment on whether it should identify a broader set of patients for whom the requirement should apply and if so, how to implement the requirement in a way that minimizes burden on hospitals**.

With respect to identifying practitioners and providers that have an established care relationship with the patient for notification, CMS suggests that hospitals may identify appropriate recipients through various methods. Information may be requested from patients or caregivers upon arrival or through the patient's medical record. Hospitals may develop processes to capture information director or through an intermediary that maintains information about care relationships. Asystem might allow a provider to specifically request notification for a patient. Providers are expected to comply with HIPAA privacy rules. CMS understands that a notification may be sent to a provider but technical issues beyond the hospital's control may prevent successful receipt of the notification.

Finally, CMS notes that hospitals have an existing responsibility under the CoPs to transfer or refer patients along with necessary medical information to appropriate facilities agencies or outpatient services as needed for follow-up or ancillary care. The proposed patient event notifications would be separate from the requirement regarding necessary medical information. However, the notification proposal may intersect with the discharge planning process and hospitals may wish to find ways to reduce redundancy.

Psychiatric hospitals must comply with hospital CoPs but are subject to separate requirements regarding medical records. CMS therefore proposes a separate new standard (42 CFR 482.61(f)) requiring these hospitals to send electronic patient event notification if they currently possess EHR systems with the technical capacity to general them. The language parallels the proposal for hospitals.

For CAHs, the same requirement with the same regulatory language is proposed at a new paragraph (d) at 42 CFR 485.638.

In the regulatory impact analysis section of the proposed rule, CMS estimates that the proposal would impose a minimal burden on hospitals but would greatly benefit patients overall. The costs would result from one-time implementation of the notification system, revision of policies related to discharge planning and communicating changes to affected staff.

CMS specifically seeks feedback about how these proposals for electronic patient event notification should be operationalized. Additionally, comment is sought on how CMS should implement these proposals as part of survey and certification guidance in a manner that minimizes compliance burden on hospitals, psychiatric hospitals, and CAHs while ensuring adherence with the standards. Finally, CMS requests input about a reasonable timeframe for implementation of these proposals for hospitals, psychiatric hospitals, and CAHs.

XI. RFI on Advancing Interoperability Across the Care Continuum

To inform future rulemaking, CMS seeks comment on potential strategies for advancing interoperability across care settings. The proposed rule includes a discussion of the need for interoperability to support better care coordination, discharge planning and timely transfer of essential health information, and the problem of lagging adoption by providers that were not part of the EHR Incentive Programs. In particular, CMS is concerned about the lack of health IT

adoption in post-acute care (PAC), behavioral health and home and community-based service settings.

In particular, **comments are sought on whether hospitals and physicians (who have been generally eligible for the Promoting Interoperability programs and have adopted CEHRT) 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 through the expansion of the USCDI process.** CMS is interested in whether the standardized patient assessment data elements that are implemented in CMS PAC assessment instruments in satisfaction of the IMPACT Act would be appropriate, or whether only a subset of these standardized items would be appropriate, and if so, which data elements should be prioritized. In addition, CMS wants to know what implementation timeline would be most appropriate for requiring adoption of these data elements in provider and hospital systems under the ONC Health IT Certification Program. Finally, CMS seeks comment on the administrative, development, and implementation burden that may be associated with adopting these data elements.

XII. Advancing Interoperability in Innovative Models

CMS states that it intends to use the Center for Medicare and Medicaid Innovation authority to test ways to promote interoperability across the health care spectrum. It believes that the Innovation Center models offer unique opportunities to engage with providers in innovative ways, and offers the Comprehensive Primary Care Plus model and several awards under the State Innovation Models initiative as examples of existing models focused on health information exchange and health IT investment.

Interoperability related-issues in future model development may include models that incorporate piloting emerging standards; models leveraging non-traditional data in model design (for example, data from schools, data regarding housing and data on food insecurity); and models leveraging technology-enabled patient engagement platforms. The Innovation Center has incorporated non-clinical data in prior models but anticipates addressing additional uses and types of non-clinical data in future models.

Comments are sought on the following general principles around interoperability within Innovation Center models for integration into new models, through provisions in model participation agreements or other governing documents. In applying these general principles, CMS intends to be sensitive to the details of individual model design as well as the characteristics and capacities of model participants. **Additionally, the Innovation Center is requesting public comment on other ways in which the Innovation Center may further promote interoperability among model participants and other health care providers aspart of the design and testing of innovative payment and service delivery models.**

1. Provide Patients Access to their Own Electronic Health Information. Certain Innovation Center models already require that participants with direct patient interactions provide their patients with electronic access to their health information within 24 hours of any encounter. New Innovation Center models may also require that providers and other health care entities with direct patient interactions provide patients access to their own electronic health information and, upon the patient's authorization, to third party developers via APIs.

2. Promote Trusted Health Information Exchange. Innovation Center model participants may, where appropriate, be required to participate in a trusted exchange network that meets the following criteria:

- The trusted exchange network must be able to exchange PHI in compliance with all applicable state and federal laws across jurisdictions.
- The trusted exchange network must connect both inpatient EHRs and ambulatory EHRs.
- The trusted exchange network must support secure messaging or electronic querying by and between patients, providers and payers.

Additionally, model participants may be required to participate in electronic alerting via one of the standards described in the ISA, II-A: Admission, Discharge, and Transfer published and updated by ONC.

3. Adopt Leading Health IT Standards and Pilot Emerging Standards. Innovation Center model participants, along with their health IT vendors, may pilot new FHIR standards and advance adoption of new data classes in USCDI (e.g., psychosocial data) to improve interoperability for care management, quality reporting or other priority use cases. The Innovation Center anticipates taking on a leadership role in developing new or less mature FHIR and supporting more innovative interventions undertaken by states, whenever possible.

XIII. RFI on Policies to Improve Patient Matching

CMS says that stakeholders have long identified the lack of a unique patient identifier (UPI) as a constraint on safe and secure electronic exchange of health information for patient. While HIPAA required adoption of a UPI, concerns about privacy and security resulted in a Congressional prohibition on the use of federal funds to engage in rulemaking to adopt a UPI standard since 1999. However, beginning in 2017 Congress has encouraged HHS, through CMS and ONC, to examine options involving patient matching as means of promoting exchange of patient health information. CMS notes that in January 2019 the Government Accountability Office (GAO) released a study on this issue that was required by section 4007 of the Cures Act.[10]

This proposed rule includes a Request for Information on policies to improve patient matching. The specific questions follow. **CMS specifically seek input on the following questions and the potential authority for the requirement:**

1. Should CMS require Medicare FFS and the payers that would be regulated under this proposed rule (MA Plans, Medicaid FFS, Medicaid managed care plans, CHIP FFS, CHIP managed care entities, and QHP issuers in FFEs (not including SADP issuers)), to use a patient matching algorithm with a proven success rate of a certain percentage where the algorithm and real world processes associated with the algorithm used are validated by HHS or a third party?

2. Should CMS require these organizations to use a particular patient matching software solution with a proven success rate of a certain percentage validated by HHS or a third party?

3. Should CMS expand the recent Medicare ID card efforts by requiring a CMS-wide identifier which is used for all beneficiaries and enrollees in health care programs under CMS

[10] GAO. Health Information Technology: Approaches and Challenges to Electronically Matching Patients' Records across Providers. January 15, 2019. https://www.gao.gov/assets/700/696426.pdf.

administration and authority? Specifically, should it require use of the Medicare ID by any or all of the following:

- MA organizations, Part D prescription drug plan sponsors, entities offering cost plans under section 1876 and other Medicare health plans.
- State Medicaid and CHIP agencies for dual eligible individuals (when feasible).
- QHP issuers in FFEs for their enrollees in the administration of their plans.

4. Should CMS advance more standardized data elements across all appropriate programs for matching purposes, perhaps leveraging the USCDI proposed by ONC for HHS adoption at 45 CFR 170.213?

5. Should CMS complement CMS data and plan data in the payers that would be regulated under this proposed rule with one or more verifying data sources for identity proofing? What potential data source should be considered? What are possible restrictions or limitations to accessing such information?

6. Should CMS support connecting EHRs to other complementary verifying data sources for identity proofing? What potential data source should be considered? What are possible restrictions or limitations to accessing such information?

7. To what extent should patient-generated data complement the patient-matching efforts?

XIV. Regulatory Impact Analysis

CMS estimates that the aggregate costs to the health care sector resulting from this proposed rule for the period 2020 through 2024 would be $500 million. Almost all of this total, $494 million, is the estimated cost of implementing the proposed API requirements and the remaining $6 million is the cost of the proposals for changing the timing of reporting data on dual eligible beneficiaries by states. Table 4 reproduced from the proposed rule shows the $494 million estimated cost of implementing and maintaining the API requirements by program.

TABLE 4: API Costs (in millions) by Year and Program

Year	2020	2021	2022	2023	2024	Total
Full Implementation and Maintenance costs (Table 3, Row 1)	275.4	54.7	54.7	54.7	54.7	494.0
Commercial Programs (57.81%)	159.2	31.6	31.6	31.6	31.6	285.6
Medicaid and CHIP programs (17.66%)	48.6	9.7	9.7	9.7	9.7	87.2
Medicare Advantage Programs (24.53%)	67.6	13.4	13.4	13.4	13.4	121.2

The analysis discusses ways in which the different affected payers could transfer these costs to enrollees, the states and the federal government. Table 10 in the proposed rule displays these estimates.

Appendices: Selected Sections of the ONC Proposed Rule

On February 21, 2019 the Office of the National Coordinator for Health Information Technology (ONC) of the Department of Health and Human Services (HHS) officially released a proposed rule "21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program") which would implement certain provisions of the 21st Century Cures Act (P.L. 114-255), including conditions and maintenance of certification requirements for health information technology (health IT) developers and modifications to ONC's 2015 Edition health IT certification criteria.

Appendix A summarizes the portion of the ONC proposed rule relating to APIs, and Appendix B summarizes the portion relating to information blocking.

APPENDIX A.
Summary of ONC Proposed Rule
VII.B.4. Conditions and Maintenance of Certification: Application Programming Interfaces

I. Background on Application Programming Interface Standards

Section 4002 of the Cures Act requires the Secretary of HHS, through notice and comment rulemaking, to establish Conditions and Maintenance of Certification requirements for the Program. Specifically, health IT developers or entities must adhere to certain Conditions and Maintenance of Certification requirements concerning application programming interfaces (APIs) and other elements. ONC's approach in the proposed rule is to use the Conditions and Maintenance of Certification to express both initial requirements for health IT developers and their certified Health IT Module(s) as well as ongoing requirements that must be met by both health IT developers and their certified Health IT Module(s) under the Program.

To implement the Cures Act's API Condition of Certification, ONC proposes new standards, new implementation specifications, and a new certification criterion as well as detailed Conditions and Maintenance of Certification requirements. The Base EHR definition would also be modified.

By ONC's description, APIs can be thought of as a set of commands, functions, protocols, or tools published by one software developer ("A") that enables other software developers to create programs and applications that interact with A's software without needing to know the "internal" workings of A's software. ONC adopted three 2015 Edition certification criteria that specify API capabilities for Health IT Modules (45 CFR 170.315(g)(7), (g)(8), and (g)(9)).

In this rule, ONC proposes to adopt standards, implementation specifications, and a new API certification criterion to implement the technical requirements associated with the Cures Act's API Condition of Certification.

II. New Standards and Implementation Specifications for APIs

As a Condition of Certification (and Maintenance thereof) under the Program, the Cures Act requires health IT developers to publish APIs that allow "health information from such technology to be accessed, exchanged, and used without special effort through the use of APIs or successor technology or standards, as provided for under applicable law." The Cures Act's API Condition of Certification also states that a developer must, through an API, "provide access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws."

ONC notes that these provisions include key phrases and requirements for health IT developers that go beyond just the technical functionality of the products they present for certification. The term "without special effort" is interpreted by ONC to have three attributes applicable to all health IT developers seeking certification:

- Standardized. The same technical API capabilities would be used.
- Transparent. Business and technical documentation necessary to interact with the APIs in production would be freely and publicly accessible.
- Pro-competitive. Business practices would promote efficient access, exchange, and use of electronic health information (EHI) to support a competitive marketplace that enhances consumer value and choice. ONC states that health IT developers must not interfere with a health care provider's use of their acquired API technology in any way, especially ways that would impact its equitable access and use based on (for example) another software developer's size, current client base, or business line. Developers together with health care providers that deploy APIs are accountable to patients who should be able to access their EHI via any API-enabled app they choose without special effort, including without incurring additional costs and without encountering access requirements that impede their ability to access their information in a persistent manner.

Key terms would be defined in the proposed regulatory text at 45 CFR 170.102: "API Technology Supplier," "API Data Provider," and "API User." In addition, ONC uses the term "API technology" to generally refer to the capabilities of certified health IT that fulfill the proposed API certification criteria at §170.315(g)(7) through (11). The term "(g)(10)-certified API" refers to health IT certified to the proposed criterion at §170.315(g)(10), and the term "app" refers to any software designed to interact with (g)(10)-certified APIs.

A. New API standards at 45 CFR 170.215

ONC proposes to add a new 45 CFR 170.215 with the following standards and associated implementation specifications for APIs as summarized here.

(a)(1) *Adoption of FHIR Standard*. ONC proposes at §170.215(a)(1) to adopt the HL7® Fast Healthcare Interoperability Resources (FHIR®) standard as a foundational standard for its proposals. Specifically, FHIR Draft Standard for Trial Use (DSTU) 2 (hereafter referred to as "FHIR Release 2") is proposed as a baseline standard conformance requirement. While the 2015 Edition final rule did not include specific standards or implementation specifications, industry was encouraged to coalesce around a standardized specification for its API functionality, such as the FHIR standard. ONC reports that 32% of developers have published their use of FHIR Release 2; 51% appear to be using a version of FHIR and OAuth 2.0[11] together. It estimates that 87% of hospitals and 57% of clinicians are served by developers with a FHIR Release 2 API and 87% of hospitals and 69% of clinicians are served by developers with any version of an FHIR API.

Because it is used in the 2015 Edition systems that are being deployed, ONC believes this proposal would pose an incremental burden on IT developers to get certified, largely limited to

[11]The proposed rule does not describe OAuth 2.0. A Google search identifies it as the industry-standard protocol for authorization used by web applications, desktop applications, mobile phones, etc. https://tools.ietf.org/html/rfc6749

the added security and registration conformance requirements that are proposed in this rule. Some developers would have to make more substantial changes, however.

Although a FHIR Release 3 is available, ONC says it is not in widespread use. However, **ONC believes that the improvements included in FHIR Release 4 mean that it will be the standard the industry would coalesce behind, and it seeks comments on several options for the final rule.**

- Option 1 is proposed in the regulatory text and would adopt just FHIR Release 2 for reference in proposed §170.315(g)(10). This would require health IT developers seeking certification to build, test, and certify systems solely to FHIR Release 2 and its associated implementation specifications. Under this option, if the National Coordinator approved the use of FHIR Release 3 or 4 (pursuant to the Standards Version Advancement Process) it would occur, at the earliest, one year after a final rule was issued. Given that timing, and the compliance deadlines proposed, health IT developers would have no option but to develop to FHIR Release 2 in order to meet the proposed compliance deadlines.
- Under Option 2, ONC would adopt both FHIR Release 2 and FHIR Release 3 with IT developers given a choice for compliance with §170.315(g)(10). Given the timing of potential approval of Release 4 health IT developers would have no option but to develop to FHIR Release 2 or Release 3 in order to meet the proposed compliance deadlines.
- Option 3 would adopt FHIR Release 2 and FHIR Release 4 with health IT developers given a choice for compliance with §170.315(g)(10). ONC sees this as the best option for the industry, but implementation depends on all applicable corresponding FHIR Release 2 implementation specifications also being published in their FHIR Release 4 formats and available prior to the issuance of a final rule. Unlike Options 1 and 2, the Standards Version Advancement Process would not be necessary for this option. ONC also seeks comment on a variant of Option 3 that would include a pre-defined cut-over for the permitted use of and certification to FHIR Release 2. If this variant were implemented, ONC would likely also need to add a maintenance of certification requirement in the final rule to establish an upgrade timeline to FHIR Release 4 for those health IT developers who originally sought certification for FHIR Release 2.
- Option 4 would adopt only FHIR Release 4 in the final rule for reference in proposed §170.315(g)(10). Developers seeking certification would be required to build, test, and certify systems solely to FHIR Release 4 and its associated implementation specifications. Again, finalizing this option is dependent on all applicable FHIR Release 4 implementation specifications being published in time for a final rule. ONC believes that by the time a final rule associated with these proposals is issued, health IT developers would have close to or more than a year's worth of development experience with FHIR Release 4.[12] Many may be poised to introduce FHIR Release 4 products into production. If ONC were to offer certification to FHIR Release 2 (as in Option 3) this flexibility could unintentionally delay the industry's transition to FHIR Release 4.

[12] As an example, compliance timeline ONC states that if the final rule were effective January 2020, developers would have until January 2022 to rollout (g)(10)-certified API technology. At that point, FHIR Release 4 would have been available for nearly 3 years.

ONC notes that if it adopts a FHIR Release in the final rule other than or in addition to Release 2, it would also adopt applicable implementation specifications and FHIR profiles in order to support US Core Data for Interoperability (USCDI) data access. (FHIR profiles are additional rules about which elements must be used and which have been added that are not part of the base FHIR resource,) **Commenters are highly encouraged to explicitly note their preferred option.**

(2) *Implementation specifications. API Resource Collection in Health (ARCH) Version 1*. This proposal for new §170.215(a)(2) lists a set of base FHIR resources that Health IT Modules certified to the proposed §170.315(g)(10) would need to support. The ARCH would align with the proposed USCDI standard. The ARCH would require 15 FHIR resources, 13 of which ONC says it knows map to and support the equivalent data classes specified in the USCDI: AllergyIntolerance; CarePlan; Condition; Device; DiagnosticReport; Goal; Immunization; Medication; MedicationOrder; MedicationStatement; Observation; Patient; and Procedure. For the patient resource it proposes to include Patient.address and Patient.telecom elements. For the device resource, device.udi element would be included.

The proposed two resources in addition to these 13 are Provenance and DocumentReference. It believes the latter is best capable of handling the exchange of clinical notes and that stakeholders have frequently indicated are important data to exchange. ONC clarifies that the clinical note text would need to be represented in its raw text form and not converted from another file or format (e.g., a PDF). With respect to the Provenance resource ONC argues that it is best to include this requirement now as it would be more burdensome to add it in the future. The Provenance.recorded (author's time stamp) and Provenance.agent.actor (author and organization) elements would be required.

ONC expects to update this implementation standard over time as the USCDI is expanded. ONC also notes that under its proposed rule (the Standards Version Advancement Process proposals), developers could voluntarily update their certified health IT to include (g)(10)-certified API access to a broader set of data once a new version of the ARCH is approved.

(3) *Implementation specifications – FHIR profiles*. ONC proposes to adopt in §170.215(a)(3) the Argonaut Data Query Implementation Guide version 1.0.0 (Argonaut IG) hosted by HL7. It specifies FHIR profile constraints for 13 of the FHIR resources proposed for the ARCH Version 1.

(4) *Implementation specifications – FHIR server conformance*. Proposed §170.215(a)(4) would require adoption of The Argonaut Data Query Implementation Guide Server conformance requirements. While this is a specific portion of the Implementation Guide and covered by adoption of the guide, ONC elects to explicitly propose this requirement because it is essential that all FHIR servers are consistently configured to support the defined data queries and searches. ONC notes that the Server IG includes conformance requirements for the "DocumentReference Profile," a specification produced in support of the 2015 Edition certification criterion adopted in §170.315(g)(9). As a result, ONC clarifies that this specific

portion of the Server IG and conformance requirement would be out of scope for the purposes of proposed §170.315(g)(10).

(5) *Implementation specification – Application authorization.* At proposed §170.215(a)(5) ONC would require support of the SMART Application Launch Framework Implementation Guide Release 1.0.0, including mandatory support for "refresh tokens," "Standalone Launch," and "EHR Launch" requirements. ONC says this guide is referenced by the Argonaut IG and is generally being implemented in the health IT community as a security layer within FHIR deployment. Three components are specified for support. ONC believes "refresh tokens" is needed to enable persistent access by apps in a patient access context; a minimum refresh token life of 3 months would apply. Standalone launch and (from a smartphone or browser outside the EHR) and within-EHR launch would both need to be supported.

ONC notes that by separately proposing the FHIR standard and implementation specifications, it may evaluate industry progress and possibly update each separately in the future. It plans to coordinate with other agencies that may be adopting the FHIR standard and implementation guides.

(b) *Application authentication*. *Standard*. To support user authentication and app authorization processes, ONC proposes at §170.215(b) to adopt the OpenID Connect Core 1.0 incorporating errata set 1 standard, which it says complements the SMART Guide. The OpenID standard is usually paired with OAuth2.0 and focuses on user authentication.

B. New API Certification Criteria at 45 CFR 170.315(g)(10)

ONC proposes new API certification criterion at §170.315(g)(10) to replace the existing criterion set forth at §170.315(g)(8). It says the current criteria need to be replaced because they focus on a Health IT Module's ability to provide API functionality that can respond to data categories specified in the Common Clinical Data Set. Current requirements at (g)(7) and (g)(9) would remain unchanged because they do not prescribe specific technical approaches that need to be replaced. By placing the new criteria separately (as opposed to modifying (g)(8)) it would be easier for industry to distinguish compliance requirements.

The proposed new API certification criterion would require FHIR servers to support API-enabled services for which a single patient's data is at focus and services for which multiple patients' data are at focus ("population-level"). API services that focus on a single patient would include those that interact with software applications controlled and used by a patient to access their data as well as software applications implemented by a provider to enhance their own "internal" clinical care tools and workflow. Most of these types of interactions are typically orchestrated in a synchronous, real to near-real-time mode via APIs. By contrast, population-level API services would include software applications used by a health care provider to manage various internal patient populations as well as external services to support a provider's quality improvement, population health management, and cost accountability vis-à-vis health plans and other partners.

Population-level uses may range from a small group to many hundreds or thousands of patients. ONC expects that such access and associated privacy and security protocols would be established consistent with existing legal requirements under the HIPAA Privacy and Security Rules and other applicable state or federal laws. For the purposes of the proposed certification criterion, ONC seeks to ensure through testing and certification that a set of baseline API functionalities exists and is deployed for providers to use at their discretion to support their own clinical priorities and to engage with their partners. ONC notes that FHIR Release 4 includes technical specifications to support standardized population-level services in a more efficient manner than is currently possible and if Options 3 or 4 for the FHIR standard described above are selected or Release 4 is approved under the Standards Version Advancement process, it could be used to meet these technical expectations. Finally, ONC says inclusion of a population-level API conformance requirement in the criterion would allow these capabilities to be evaluated post-certification for compliance with this criterion and the information blocking and real-world testing conditions of certification.

Under the Standardized API for patient and population services Condition of Certification criterion proposed at §170.315(g)(10) API technology would need to meet the following technical requirements for certification. All data elements indicated as mandatory would be in scope for testing.

(i) *Data response*. The technology would have to be capable to respond to requests for data (based on an ID or other token) for each of the FHIR resources in ARCH Version 1 and consistent with FHIR Release 2 and the Argonaut IG implementation specification.

(ii) *Search support*. The technology would have to be capable of responding to all supported searches identified in the Argonaut Data Query Implementation Guide Server (proposed at §170.215(a)(4)). For population-level searches a developer would be permitted to choose the most efficient manner because there is not a standardized specification for FHIR services to handle searches for multiple patients. **ONC seeks comment on the minimum search parameters that would need to be supported for the DocumentReference and Provenance resources, which are currently included in the base FHIR standard.**

(iii) *App registration*. The technology would be required to be capable of enabling apps to register with the technology's "authorization server." The API Technology Supplier would have to demonstrate its registration process, but ONC would not require that it be done according to a specific standard. **ONC seeks public comment on whether it should require the OAuth 2.0 Dynamic Client Registration Protocol (RFC 7591) standard ("Dynamic Registration") as the only way to support registration for this certification criterion.** ONC considered proposing Dynamic Registration as a requirement but did not do so because it has not been widely adopted. It believes it is more prudent to require the function and let the industry reach consensus on the best techniques to enable registration. ONC notes that a specific "maintenance requirement" associated with the API Condition of Certification around the timeliness of this registration process is proposed to ensure that patients can use their apps in a timely manner. (See discussion of §170.404(b) below.) **ONC requests comment on its plan to not test registration capabilities for apps that would be executed within an API Data Provider's**

clinical environment because it believes that API Technology Suppliers and API Data Providers are best poised to innovate and execute various methods for app registration within a clinical environment.

(iv) *Secure connection*. The technology would be required to demonstrate capability to establish a secure and trusted connection with an application that requests data in accordance with the SMART Guide. This would require that an authorization server be used and that it support at least "authorize" and "token" endpoints and the publication of the endpoint URLs via FHIR server's metadata as specified in the SMART Guide. Initial conformance would focus on secure connection parameters for a single patient's data and the developer could approach secure connections for multiple patients as it deems most efficient to meet the proposed certification criterion.

(v) *Authentication and app authorization – 1st time connection*. The first time an application connects to request data the technology would have to demonstrate that user authentication occurs during the process of authorizing the application to access FHIR resources in accordance with the OpenIDConnect Core 1.0 incorporating errata set 1 standard. ONC notes that this standard is agnostic to the authentication mechanism itself. Further, the technology would be required to demonstrate that a user can authorize applications to access data in accordance with the SMART Guide and issue a refresh token that is valid for a period of at least 3 months. ONC intends to test health IT in both the Standalone Launch and EHR Launch modes. ONC clarifies that the provision does not require support for OpenID Connect Standard capabilities that are not specified in the SMART Guide. Further, it notes that the proposed refresh token requirement differs from providing an access token with extended life which is discouraged from a security standpoint.

(vi) *Authentication and app authorization – Subsequent connections*. The technology would be required to demonstrate that an application can access data without requiring re-authorization and re-authentication when a valid refresh token is supplied and issue a new refresh token for new periods no shorter than 3 months. ONC says this renewal requirement responds to stakeholder concerns that a constant need for patients to re-authenticate and re-authorize their apps creates usability challenges and may otherwise contradict the Cures Act's intent associated with the phrase "without special effort." **It seeks comment on whether there are available specifications it should review as well as whether there should be a reasonable upper bound from a timing perspective (e.g., one year) after which the user should be required to re-authenticate and re-authorize.** ONC notes that it expects FHIR Release 4 to specify handling of population-level data requests; under this proposal a developer could use any approach to these requests it deems most efficient.

(vii) *Documentation*. An API Technology Supplier would be required to include complete documentation including at a minimum:

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

- The software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s).
- All applicable technical requirements and attributes necessary for an application to be registered with an authorization server.

All documentation would have to be accessible to the public via a publicly accessible hyperlink without any additional access requirements. Prohibited for example would be requirements for registration, account creation, click-through agreements, or requirements for contact information or other information.

ONC notes that the 2015 Edition final rule included transparent documentation requirements for the API certification criteria adopted at §170.315(g)(7) through (g)(9) and proposes to modify these provisions as well as §170.315(g)(10) and (11). Specifically, it proposes to focus the documentation requirement on solely the technical documentation associated with the API technology and therefore would remove provisions associated with "terms of use" which are not technical and are more reflective of business practice. In addition, the proposed technical documentation would be broadened to require the API Technology Supplier to provide detailed information for all aspects of its (g)(10)-certified API, especially for any unique technical requirements and configurations such as optional elements of the Argonaut IG Patient Profile, for example. For aspects fully specified by the FHIR standard, hyperlinks could be provided as part of its overall documentation.

III. API Condition of Certification Requirements (§170.404)

ONC says that to implement the Cures Act it is proposing API Condition of Certification to complement the technical capabilities described above while addressing the broader technology and business context within which the API will be used. The following sections describe the requirements as proposed in §170.404. They are proposed to apply to developers of Health IT Modules certified to *any* of the criteria under current and proposed §170.315(g)(7) through (11). ONC notes that the proposed policies would not apply to a health IT developer's practices associated with criteria that are not one of the API-focused criteria but says that developers should be mindful that other provisions of the proposed rule, such as information blocking, could still apply to the non-API-focused certification criteria.

(a) *Condition of Certification*. (1) *General.* An API Technology Supplier would be required to publish APIs and to allow health information from APIs to be accessed, exchanged, and used without special effort using APIs or successor technology or standards, as provided for under applicable law, including providing access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws. By the term "all data elements" ONC means the scope of the ARCH and its associated implementation specifications and the policy expressed around the data elements that must be supported by (g)(10)-certified APIs. ONC expects that these APIs will be able to support access to more data over time as the USCDI and the ARCH are updated.

(2) *Transparency conditions*. ONC proposes that the business and technical documentation published by an API Technology Supplier must be complete and published via a publicly accessible hyperlink that allows any person to directly access the information without any preconditions or additional steps. The published documentation would have to include all terms and conditions for the API technology, including any restrictions, limitations, obligations, registration process requirements, or other similar requirements that would be needed to:

- Develop software applications to interact with the API technology;
- Distribute, deploy, and enable the use of software applications in production environments that use the API technology;
- Use software applications, including to access, exchange, and use electronic health information by means of the API technology;
- Use any electronic health information obtained by means of the API technology; and
- Register software applications.

Any and all fees charged by an API Technology Supplier for the use of its API technology would have to be described in detailed, plain language. The description of the fees must include all material information, including the persons or classes of persons to whom the fee applies; the circumstances in which the fee applies; and the amount of the fee, which for variable fees must include the specific variables and methodologies used to calculate the fee.

ONC proposes a compliance date of six months from the final rule's effective date for developers with products already certified to §170.315(g)(7),(8) or (9) to meet the specific transparency conditions. In addition, it recognizes that API Technology Suppliers will need to update the publicly available information from time to time. ONC expects suppliers to make clear to the public the timing of their disclosures in order to prevent discrepancies between information in its public documentation and what it may be communicating directly to customers.

Under the proposed rule, an API Technology Supplier would be permitted to institute a process to verify the authenticity of application developers so long as such process is objective and the same for all application developers and completed within 5 business days of receipt of an application developer's request to register their software application for use with the API Technology Supplier's API technology. ONC notes that this proposal is needed because it did not propose to adopt the Dynamic Registration standard in (g)(10). **ONC seeks comments on factors that would enable registration with minimal barriers,** such as allowing suppliers to do one-time verification of app developers. However, it is concerned about the potential for a malicious app developer to spoof the app of another and other trade-offs. Under the proposal suppliers would have the discretion to develop a verification process as long as it is objective and the same for all developers and reasonably completed within the five business days. **Comments are requested on other timing considerations.**

The use of an application developer verification process would be optional, and ONC reminds stakeholders that even when an API Technology Supplier chooses not to use such a process, apps would not have carte blanche access to a health care provider's data. They would still be

registered and could be de-activated by an API Technology Supplier or health care provider if they behave in anomalous or malicious ways. A patient seeking access to their data using the app will have to authenticate themselves, authorize the app to connect to the FHIR server and specify the scope of data which the app may access.

ONC notes that, separate from this provision, API Technology Suppliers may establish additional mechanisms to vet app developers. Such mechanisms could fit into the "value-added services" permitted fee and result in the app being acknowledged or listed by the health IT developer in some special manner (e.g., in an "app store," "verified app" list). No explicit limits to the nature of these approaches are specified but ONC cautions that in addition to offering an extra layer of trust they can be used to prevent, limit, or otherwise frustrate innovation, competition, and access to the market. This use could directly violate the specific condition of certification associated with fees permitted for value-added services and could constitute information blocking.

(3) *Permitted fees conditions*. In general, an API Technology Supplier would be prohibited from imposing any fees, but certain permitted fees would be allowed, and these are described below. The prohibition is meant to ensure that Suppliers do not engage in pricing practices that create barriers to entry and competition for apps that health care providers seek to use. The permitted fees are intended to recognize that suppliers need to recover costs and earn a reasonable return for providing certified API technology. ONC emphasizes that fees would not be allowed in any way in connection with a supplier's work to support use of API technology to facilitate a patient's ability to access, exchange or use their EHI. Other than those for value-added services, fees would always be between an API Technology Supplier and an API Data Provider. However, ONC notes that the conditions do not address who may pay the fee, although this may be affected by other federal or state laws and regulations addressing relationships involving remuneration. ONC notes that the proposed "permitted fees conditions" described below align with the requirements of the information blocking exceptions proposed in 45 CFR 171.204 and 171.206. (The Information Blocking provisions are summarized in Appendix B of this document.)

For any permitted fee imposed by an API Technology Supplier on an API Data Provider, several general assurances would be required. First, a Supplier would be required to ensure that the fee was based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests. Second, the fees imposed would need to be reasonably related to the Supplier's costs of supplying and supporting API technology to the user being charged. For example, a fee would not be permitted if the underlying costs had already been recovered. ONC states further that a supplier that conditioned access to API technology on revenue sharing or entry into a royalty agreement would be at risk of violating this condition. Third, the costs of supplying and supporting the API technology upon which the fee is based would have to be reasonably allocated among all the supplier's customers using the technology. For example, the supplier could not recover the total of its core costs from each customer. However, costs unique to a customer would not have to be distributed among customers. Finally, fees could not be based in any part on whether the requestor or other person is a competitor, potential competitor, or will be using the API technology in a way that facilitates

competition with the supplier. **ONC requests comments on these conditions for permitted fees and whether it has provided sufficient guardrails to ensure that fees do not prevent EHI from being accessed, exchanged and used through APIs without special effort.**

ONC reminds readers that the scope of API technology subject to the proposals includes only certified health IT that fulfill the current or proposed certification criteria at §170.315(g)(7) through (11). Other API functionality provided by a supplier would not be subject to the condition of certification proposed at §170.404.

The following permitted fees are proposed. In addition to satisfying one of the proposed permitted fees, the general conditions described above would apply.

Permitted fee – Development, deployment, and upgrades. An API Technology Supplier would be permitted to charge fees to an API Data Provider to recover the costs reasonably incurred by the API Technology Supplier to develop, deploy, and upgrade API technology for the API Data Provider. Fees for developing API technology could not include the supplier's costs of updating non-API related capabilities, including its databases, as part of its development of the API technology because ONC says this would be inconsistent with the Cures Act requirement that API technology be deployed "without special effort." Fees for "deploying" API technology comprise supplier's costs of operationalizing API technology in a production environment and include standing up hosting infrastructure, software installation and configuration, and the creation and maintenance of API Data Provider administrative functions. These fees would not include the costs associated with managing the traffic of API calls that access the API technology, which a supplier can only recover under the permitted fee for usage support costs described immediately below. For the purpose of this Condition of Certification, ONC considers API technology to be "deployed" by the customer—the API Data Provider—that purchased or licensed it. Fees for "upgrading" API technology comprise the supplier's costs of supplying a provider with an updated version of API technology, such as the costs required to bring API technology into conformity with new program requirements, upgrades to implement general software updates (not otherwise covered by development fees or under warranty), or developing and releasing newer versions of the API technology at the request of an API Data Provider. Costs would depend on the scope of work undertaken by the supplier. ONC proposes that any fees under this category of permitted fees could be charged only to the data provider(s) for whom the capabilities are deployed. It expects the fees would be negotiated between these parties. ONC believes it would be inappropriate to pass the costs on to API Users.[13]

Permitted fee – Supporting API uses for purposes other than patient access. An API Technology Supplier would be permitted to charge usage-based fees to an API Data Provider to recover the incremental costs reasonably incurred by the supplier to support the use of API technology deployed by or on behalf of the provider. This permitted fee could not include:

[13] Under the definitions proposed at 170.102, an API User creates software applications that interact with the APIs developed by the API Technology Supplier, and an API Data Provider is the organization that deploys the API technology (e.g., a health care provider).

- Any costs incurred by the API Technology Supplier to support uses of the API technology that facilitate a patient's ability to access, exchange, or use their electronic health information;
- Costs associated with intangible assets (including depreciation or loss of value), except the actual development or acquisition costs of such assets; or
- Opportunity costs, except for the reasonable forward-looking cost of capital.

ONC expects that usage support fees would only come into play when the supplier acts on behalf of the provider to deploy the technology. The fees would include incremental costs attributable to supporting API interactions at increasing volumes and scale. ONC expects that suppliers would offer a certain number of "free" API calls and impose the usage-based fee after that threshold was exceeded, on the basis that a certain number of calls would be assumed in the costs recovered for deployment services. Suppliers might charge on a fee-per-call pricing structure, but in this case ONC cautions that the fees paid by the provider would need to be reasonably related to the supplier's costs of proving the technology. Similarly, a flat fee pricing structure would be permitted provided that the fee was reasonably related to the cost of services (i.e., a realistic estimate of the volume of calls). The usage fees could not include any costs associated with preparing to get the technology up and ready for use. A fee to cover these costs would be permitted under the development, deployment, and upgrades fee described immediately above.

ONC reiterates the general prohibition on fees associated with the access, exchange, and use of EHI by patients. This prohibition is based on the view that fees between a supplier and provider would likely be passed on directly to patients, creating a significant impediment to their ability to access, exchange, and use their EHI, without special effort, through applications and technologies of their choice. ONC also believes that patients have effectively paid for most of the information contained in a patient's electronic record because it was documented in the course of providing health care services to patients, and it would be inappropriate to charge patients additional costs to access this information, whether charged directly or passed on as a result of fees charged to persons that provide apps, technologies, and services on a patient's behalf. ONC notes that any unreasonable fees associated with a patient's access to their EHI may be suspect under the information blocking provision and inconsistent with an individual's right of access to their PHI under the HIPAA Privacy Rule.

ONC also proposes to explicitly exclude two additional costs from this permitted fee. The fee could not include costs associated with intangible assets (including depreciation or loss of value), except the actual development or acquisition costs of such assets. Nor could the fee include opportunity costs, which ONC considers speculative except for the reasonable forward-looking cost of capital.

Permitted fee – Value-added services. An API Technology Supplier would be permitted to charge fees to an API User for value-added services supplied in connection with software that can interact with the API technology, provided that such services are not necessary to efficiently and effectively develop and deploy such software. These value-added services would need to be provided in connection with and supplemental to the development, testing, and deployment of software applications that interact with API technology. ONC emphasizes that fees would not be

permitted if they interfere with an API User's ability to develop and deploy production-ready software. A fee would only be permitted if it relates to a service that a software developer can elect to purchase. ONC believes this type of fee is appropriate because API Technology Suppliers may offer a wide-range of market differentiating services to API Users such as advanced training, premium development tools and distribution channels, and enhanced compatibility/integration testing assessments. However, suppliers are cautioned that API value-added services would have to be made available in a manner that complies with other requirements of this Condition of Certification and with the information blocking provision. Examples of permitted and not-permitted activities under this fee are offered in the proposed rule.

Prohibited Fees. ONC says it continues to receive evidence that some health IT developers are engaging in practices that create special effort when it comes to API technology. These practices include fees that create barriers to entry or competition as well as rent-seeking and other opportunistic behaviors. For this reason, the proposed rule identifies the following examples of prohibited fees.

- Any fee for access to the documentation that an API Technology Supplier is required to publish or make available under the Condition of Certification.
- Any fee for access to other types of documentation or information that a software developer may reasonably require to make effective use of API technology for any legally permissible purpose.
- Any fee in connection with any services that would be essential to a developer or other person's ability to develop and commercially distribute production-ready applications that use API technology. These services could include, for example, access to "test environments" and other resources that an app developer would need to efficiently design and develop apps or access to distribution channels necessary to deploy production-ready software and to production resources, such as the information needed to connect to FHIR servers (endpoints) or the ability to dynamically register with an authorization server.

Permitted Fees Request for Comment. **ONC requests comment on any additional specific "permitted fees" that API Technology Suppliers should be able to recover in order to assure a reasonable return on investment.** Furthermore, the agency requests comment on whether it would be prudent to adopt specific, or more granular, cost methodologies for the calculation of the permitted fees. Commenters are encouraged to consider, in particular, whether the approach ONC has described will be administrable and appropriately balance the need to ensure that patients, providers, app developers, and other stakeholders do not encounter unnecessary costs and other special effort with the need to provide adequate assurance to API Technology Suppliers, investors, and innovators that they will be able to earn a reasonable return on their investments in API technology. ONC welcomes comments on whether the approach adequately balances these concerns or would achieve its stated policy goals, and it welcomes comments on potential revisions or alternative approaches. Detailed comments are encouraged to include, where possible, economic justifications for suggested revisions or alternative approaches.

Permitted Fees Record-keeping Requirements. An API Technology Supplier would be required to keep for inspection detailed records of any fees charged with respect to the API technology, the methodologies used to calculate such fees, and the specific costs to which such fees are attributed. Separately, an API Technology Supplier would need to document the criteria it used to allocate any costs across relevant customers, requestors, or other persons. The criteria must be documented in a level of detail that would enable determination as to whether the supplier's cost allocations are objectively reasonable and comply with the cost accountability requirements. ONC notes that the supplier would have to meet the records retention requirement proposed elsewhere in the proposed rule as part of the Assurances Condition of Certification (proposed for adoption in §170.402). **ONC requests comment on whether these requirements provide adequate traceability and accountability for costs permitted under this API Condition of Certification**. Comments are also requested on whether to require more detailed accounting records or to prescribe specific accounting standards.

(4) *Openness and pro-competitive conditions*. *General condition.* An API Technology Supplier would be required to grant an API Data Provider the sole authority and autonomy to permit API Users to interact with the API technology deployed by the provider. More specific provisions are also proposed as summarized below, and ONC says these proposed conditions are intended to provide clear rules and expectations for API Technology Suppliers. ONC notes that the API technology required by this Condition of Certification is subject to strict protections under the information blocking provision. To the extent that API Technology Suppliers claim an intellectual property right or other proprietary interest in the API technology, ONC admonishes that they must take care not to impose any fees, require any license terms, or engage in any other practices that could add unnecessary cost or other burden that could impede the effective use of the API technology for facilitating access, exchange, or use of EHI. Moreover, ONC believes that, as developers of technology certified under the Program, API Technology Suppliers owe a special responsibility to patients, providers, and other stakeholders to make API technology available in a manner that is truly open and minimizes any costs or other burdens that could result in special effort.

- Non-discrimination. An API Technology Suppler would be required provide API technology to API Data Providers on terms that are no less favorable than it provides to itself and its own customers, suppliers, partners, and other persons with whom it has a business relationship. The terms would have to be based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests. Different terms or service could not be offered on the basis of whether the API User with whom a provider has a relationship is or could be a competitor; or whether the revenue or other value the API User with whom an API Data Provider has a relationship may derive from access, exchange, or use of electronic health information obtained by means of API technology.
- Rights to access and use API technology. An API Technology Supplier would be required to have and grant upon request to API Data Providers and their API Users all rights that may be reasonably necessary to access and use API technology in a production environment. The proposal would not extend to intellectual property of the supplier that

has no nexus with the access and use of API technology. Suppliers would need to grant rights that could include the following to support use of the API technology:

- For the purposes of developing products or services designed to be interoperable with the supplier's health information technology or with health information technology under the supplier's control;
- Any marketing, offering, and distribution of interoperable products and services to potential customers and users that would be needed for the API technology to be used in a production environment; and
- Enabling the use of the interoperable products or services in production environments, including accessing and enabling the exchange and use of electronic health information.

None of the rights described above could be conditioned on a requirement that the recipient of the rights do, or agree to do, any of the following:

- Pay a license fee, royalty, or revenue-sharing arrangement for such rights.
- Not compete with the API Technology Supplier in any product, service, or market.
- Deal exclusively with the API Technology Supplier in any product, service, or market.
- Obtain additional licenses, products, or services that are not related to or can be unbundled from the API technology.
- License, grant, assign, or transfer any intellectual property to the API Technology Supplier.
- Meet additional developer or product certification requirements.
- Provide the API Technology Supplier or its technology with reciprocal access to application data.

ONC notes that these prohibitions mirror those proposed under exceptions to the information blocking definition but offers an important distinction in that under the API Condition of Certification would not permit any royalty, license fee or other type of fee whereas the information blocking definition would permit a developer to charge a reasonable royalty to license interoperability elements. The different treatment is due to the statutory requirement that APIs facilitate access exchange and use of patient information from EHRs "without special effort."

- Service and support obligations. An API Technology Supplier would be required to provide all support and other services reasonably necessary to enable the effective development, deployment, and use of API technology by API Data Providers and their API Users in production environments. The following obligations are specified:
  - Changes and updates to API technology: A supplier would have to make reasonable efforts to maintain the compatibility of its API technology and to otherwise avoid disrupting the use of API technology in production environments.
  - Changes to terms and conditions: Except as exigent circumstances require, prior to making changes or updates to its API technology or to the terms and conditions, a supplier would have to provide notice and a reasonable opportunity for its data provider customers and registered application developers

to update their applications to preserve compatibility with API technology and to comply with applicable terms and conditions.

ONC clarifies that this requirement would not prevent a supplier from making improvement to its technology, but the supplier would need to demonstrate that its actions were necessary and that it afforded the licensee a reasonable opportunity to update its technology to maintain interoperability. ONC recognizes that an API Technology Supplier may have to suspend access or make other changes immediately and without prior notice in response to legitimate privacy, security, or patient safety-related exigencies, and these actions would be permitted provided they do not unnecessarily interfere with the use of API technology. The overlap between these provisions and information blocking requirements are discussed in the proposed rule.

(b) *Maintenance of Certification*. (1) *Registration for production use.* An API Technology Supplier with (g)(10)-certified health IT would have to register and enable all applications for production use within 1 business day of completing its verification of an application developer's authenticity (as described in the application developer verification provision above). ONC believes this proposed requirement is needed to ensure that a patient's ability to use an app of their choice is not slowed by a supplier, causing special effort by the patient to access their EHI. A supplier that chooses not to engage in developer verification would need to meet this one business day requirement from the point of having received a request for registration.

(2) *Service Base URL publication*. An API Technology Supplier would have to support the publication of Service Base URLs for all its customers, regardless of those that are centrally managed by the API Technology Supplier or locally deployed by an API Data Provider and make such information publicly available (in a computable format) at no charge. In order to interact with a FHIR RESTful[14] API, an app needs to know the FHIR Service Base URL, also called the FHIR server's endpoint. To enhance the ease with which Service Base URLs could be obtained and used, ONC strongly encourages suppliers, providers, health information networks and patient advocacy organizations to coalesce around the development of a public resource or service from which all stakeholders could benefit.

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

In addition, ONC proposes to add compliance timeline language to the 2015 Edition Base EHR definition in §170.102 to provide for a transition from §170.315(g)(8) to §170.315(g)(10) that would reflect a total of 24 months from the final rule's effective date. ONC believes this approach is best because it identifies a single, specific date for both API Technology Suppliers and API Data Providers by which upgraded API technology would need to be deployed in

[14] "RESTful" interfaces" are those that are consistent with Representational State Transfer (REST) architectural style and communications approaches to web services development.

production. It believes that 24 months is enough because its proposals reflect a large portion of capabilities API Technology Suppliers have already developed and deployed to meet §170.315(g)(8). Moreover, this single date enables API Technology Suppliers (based on their client base and IT architecture) to determine the most appropriate timeline for development, testing, certification, and product release cycles in comparison to having to meet an arbitrary "must be certified by this date" requirement.

Appendix B.
Summary of ONC Proposed Rule
VIII. Information Blocking

Section 4004 of the Cures Act added section 3022 of the PHS Act to define and prohibit information blocking by health care providers, IT developers of certified health IT, health information exchanges, and heath information networks. While section 3022 defines information blocking in very broad terms, it also directs the Secretary to identify reasonable and necessary activities and practices that do not constitute information blocking. ONC identifies several activities that do not constitute information blocking, and it refers to these activities as exceptions. The exceptions would apply to certain activities that do in fact interfere with the access, exchange, or use of EHI but that may be reasonable and necessary if certain conditions are met. In the preamble, ONC distinguishes between practices and activities as follows: a practice is conduct that implicates the information blocking rule and that does not fall into one of the exceptions whereas an activity is conduct that implicates the information blocking rule but falls within an exception and meets all terms and conditions for the exception to apply.

ONC proposes seven exceptions which are described in detail below. In developing the exceptions, ONC says it was guided by three overarching policy considerations.

1. The exceptions would be limited to certain activities that clearly advance the aims of the information blocking rule; promote public confidence in health IT infrastructure by supporting the privacy and security of EHI and protecting patient safety; and promote competition and innovation in health IT and its use to provide health care services to consumers.
2. Each exception is intended to address a significant risk that health care providers, health IT developers of certified health IT, health information networks, and health information exchanges will not engage in these reasonable and necessary activities because of potential uncertainty regarding whether they would be considered information blocking.
3. Each exception is intended to be tailored, through appropriate conditions, so that it is limited to the reasonable and necessary activities that it is designed to exempt.

To qualify for any of these exceptions, an individual or entity would, <u>for each relevant activity and at all relevant times</u>, have to satisfy all of the applicable conditions of the exception. The burden of proof would be on the individual or entity to demonstrate compliance with all the conditions.

Section 3022 of the PHS Act imposes penalties for individuals or entities that commit information blocking. In the case of health IT developers of certified health IT, health information networks, and health information exchanges, violations are subject to a civil monetary penalty determined by the Secretary for all such violations, which may not exceed $1,000,000 per violation. The amount of the penalty takes into account factors such as the nature and extent of the information blocking and harm resulting from such information blocking, including, where applicable, the number of patients affected, the number of providers affected, and the number of days the information blocking persisted. For health care providers who commit information blocking, the statute requires the provider to be referred to the appropriate

agency that will determine "appropriate disincentives using authorities under applicable Federal law," as the Secretary establishes through notice and comment rulemaking. On this issue, **ONC requests information on appropriate disincentives under federal law, including modification to current penalties or disincentives, as well as on avoiding duplicate penalty structures for information blocking.**

The preamble to the proposed rule describes the legislative background and purpose of the information blocking rule. ONC proposes to add a new Part 171 to title 45 of the Code of Federal Regulations to implement the information blocking rules of section 3022. **ONC seeks comment on all aspects of its proposals to implement the information blocking rule**.

I. Information Blocking; Definitions

A. Information Blocking (§171.103)

ONC proposes to codify with only technical changes the definition of information blocking contained in section 3022(a)(1) of the PHS Act. The proposed regulation text is as follows:

> **Information blocking**. Information blocking means a practice that—
> (a) Except as required by law or covered by an exception set forth in subpart B of this part, is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information; and
> (b) If conducted by a health information technology developer, health information exchange, or health information network, such developer, exchange, or network knows, or should know, that such practice is likely to interfere with, prevent, or materially discourage the access, exchange, or use of electronic health information; or
> (c) If conducted by a health care provider, such provider knows that such practice is unreasonable and is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information.

ONC proposes to define or clarify a number of terms or concepts contained in information blocking definition.

(1) *Required by law*. ONC proposes to clarify that "required by law" specifically refers to any interference with access, exchange, or use of EHI that is explicitly required by state or federal law.

(2) *Likelihood of interference.* Noting that the information blocking rule is preventive in nature, the proposed rule prohibits practices that are likely to interfere with, prevent or materially discourage (hereafter generally referred to as interfere or interfering) access, exchange, or use of EHI. Thus, where there is a reasonably foreseeable risk that a practice will interfere with access, exchange, or use of EHI, it may violate the information blocking rule even if harm does not actually materialize.

ONC describes a number of different practices that always will, almost always will, or are likely to implicate the information blocking rule.

- Observational health information. ONC believes that a practice to interfere with access, exchange, or use of EHI in the context of observational health information will always implicate the information blocking rule. Observational health information refers to information created or maintained during the practice of medicine or the delivery of patient care, such as patient information in an electronic health record (EHR) or other clinical information management systems when it is clinically relevant, directly supports patient care, or facilitates delivery of health care to consumers. By contrast, EHI created through aggregation or algorithms that transform observational health information to fundamentally new data (such as population trends, risk scores, etc.) are not observational health information.

- Purposes for which information may be needed. ONC believes that a practice that interferes with access, exchange, or use of EHI in any of the following circumstances will almost always implicate the information blocking rule.
  - Providing patients access to their EHI and the ability to exchange and use it without special effort.
  - Ensuring health care professionals, care givers, and other authorized persons have the EHI they need, when and where they need it, to make treatment decisions and effectively coordinate and manage patient care, and can use the EHI they may receive from other sources.
  - Ensuring that 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.
  - Ensuring that health care providers can access, exchange, and use EHI for quality improvement and population health management activities.
  - Supporting access, exchange, and use of EHI for patient safety and public health purposes.

Thus, practices that increase the cost, difficulty, or other burden of accessing, exchanging, or using EHI for these purposes would almost always implicate the information blocking rule.

- Control over essential interoperability elements. ONC proposes that where an actor has substantial control over one or more interoperability elements that provide the only reasonable means of accessing, exchanging, or using EHI for a particular purpose, any practice by the actor that could impede the use of the interoperability elements—or that could unnecessarily increase the cost or other burden of using the elements—would almost always implicate the information blocking provision. ONC also cites examples of technological dependence, such as contractual and intellectual property obligations, a reluctance to switch to other technologies due to costs and workflow disruptions, and network effects of health IT adoption (where providers rely on technologies adopted by other parties with whom they must exchange EHI). ONC provides specific examples of this dependence. ONC cautions that actors with control over interoperability elements must be careful not to exclude appropriate persons from use of those elements or to create artificial costs or other impediments to that use.

- Practices likely to interfere. ONC believes the following practices are likely to implicate the information blocking provision by restricting access, exchange, or use of EHI.
  - Formal restrictions, such as license or contract terms, sharing policies, intellectual property or other rights, etc., as well as informal restrictions, such as when an actor refuses to exchange or facilitate access or use of EHI. ONC provides several examples of each.
  - Limiting or restricting the interoperability of health IT, such as disabling or restricting use of a capability that permits users to share EHI with other systems or configuring technology so that the types of data that may be exported or used is limited.
  - Impeding innovation and advancement, such as exclusionary, discriminatory, or other practices that impede development, dissemination or use of interoperable technologies and services that enhance access, exchange, or use of EHI. ONC provides several examples.
  - Opportunistic pricing practices, such as "rent-seeking" and other practices that artificially increase the cost and expense to access, exchange, or use EHI. ONC provides several examples.
  - Non-standard implementation policies of health IT that increase the complexity or burden of accessing, exchanging, or using EHI. This would occur where an actor chose not to adopt, or to materially deviate from, relevant IT standards, implementation specification, and certification criteria established by ONC or by the relevant segment of the IT industry.

B. Other definitions (§171.102)

ONC proposes to establish definitions for a number of additional terms, some of which are described below:

(1) *Actor*. ONC proposes to define the term actor to refer to health care providers, health IT developers of certified health IT, health information exchanges, and health information networks. ONC distinguishes among the types of actors in the rule when necessary.

(2) *Health care provider*. ONC proposes to use the very broad definition of health care provider established under the HITECH ACT under section 3000(3) of the PHS Act which includes all individuals and entities covered by the HIPAA definition.[15] The agency notes that a health care provider could also be operating as a different type of actor (e.g., a health information network) under certain circumstances.

[15] The term health care provider is defined to include a hospital, skilled nursing facility, nursing facility, home health entity or other long term care facility, health care clinic, community mental health center, renal dialysis facility, blood center, ambulatory surgical center, emergency medical services provider, Federally qualified health center, group practice, a pharmacist, a pharmacy, a laboratory, a physician, a practitioner (as described in section 1842(b)(18)(C) of the SSA), a provider operated by, or under contract with, the Indian Health Service or by an Indian tribe, tribal organization, or urban Indian organization, a rural health clinic, a 340B covered entity, a physical or occupational therapist or a qualified speech-language pathologist, and any other category of health care facility, entity, practitioner, or clinician determined appropriate by the Secretary.

(3) *Health Information Exchange* or *HIE.* ONC proposes to define the term to mean 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. ONC notes this would include regional health information organizations, state health information exchanges, and other types of organizations, entities, or arrangements that enable EHI to be accessed, exchanged, or used among particular types of parties or for particular purposes.

(4) *Health Information Network* or *HIN*. ONC would define the term to mean an individual or entity that satisfies one or both of the following:

- 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 EHI between or among two or more unaffiliated individuals or entities.
- Provides, manages, controls, or substantially influences 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 notes that a health care provider or other entity that enables, facilitates, or controls movement of EHI within its own organization, or among its affiliated entities, would not be considered a health information network vis-à-vis that movement of information.

(5) *Health IT developer of certified health IT.* ONC would define the term to mean an individual or entity that develops or offers health IT certified under the ONC Health IT Certification Program (Program) at the time the actor engaged in a practice that is the subject of an information blocking claim. ONC highlights that the definition would apply to individuals or entities that develop *or offer* certified health IT. ONC also notes that the information blocking rule is not limited to practices related only to certified health IT; it would apply to any practice by an individual or entity that develops or offers certified health IT that is likely to interfere with access, exchange, or use of EHI, including practices associated with any of the developer's or offeror's health IT products that have not been certified under the Program. It would also apply to claims of information blocking against a developer whose certification is terminated or withdrawn for practices that occurred during the period of the health IT's certification. ONC is considering additional approaches to ensure developers and offerors are subject to the information blocking rule for an appropriate period of time after leaving the Program. Self-developers of certified health IT (as understood under the Program) would be treated as a health care provider.

(6) *Electronic Health Information (EHI)*. ONC proposes to define this term to mean—

- Electronic protected health information (ePHI); and
- Any other information that—
  - is transmitted by or maintained in electronic media;
  - identifies an individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual; and

- relates to the past, present, or future health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

ONC notes the definition is intended to include an expansive set of EHI, and would encompass health information that is created or received by health care providers and those operating on their behalf; health plans; health care clearinghouses; public health authorities; employers; life insurers; schools; or universities.

(7) *Interoperability element.* ONC's intent is to define this term very broadly so it captures all potential means by which EHI may be accessed, exchanged or used for any relevant purpose, both now and as conditions evolve. The agency clarifies that the means of accessing, exchanging, and using EHI are not limited to functional elements and technical information but also encompass technologies, services, policies, and other conditions necessary to support the many potential uses of EHI. ONC would define the term as follows:

- Any functional element of a health IT, whether hardware or software, that could be used to access, exchange, or use EHI for any purpose, including information transmitted by or maintained in disparate media, information systems, health information exchanges, or health information networks.
- Any technical information that describes the functional elements of technology (such as a standard, specification, protocol, data model, or schema) and that a person of ordinary skill in the art may require to use the functional elements of the technology, including for the purpose of developing compatible technologies that incorporate or use the functional elements.
- Any technology or service that may be required to enable the use of a compatible technology in production environments, including any system resource, technical infrastructure, or health information exchange or health information network element.
- Any license, right, or privilege that may be required to commercially offer and distribute compatible technologies and make them available for use in production environments.
- Any other means by which EHI may be accessed, exchanged, or used.

C. Price information not defined

ONC does not propose a definition of the term price information but, noting that it "has a unique role" in possibly establishing a framework to prevent the blocking of price information, **it seeks comment on the technical, operational, legal, cultural, environmental and other challenges to creating price transparency within health care**.

II. Exceptions for Reasonable and Necessary Activities That Do Not Constitute Information Blocking

Consistent with section 3022, ONC proposes seven exceptions that would apply to certain activities that do in fact interfere with the access, exchange, or use of EHI (i.e., constitute information blocking) but that are reasonable and necessary if certain conditions are met.

The first three exceptions address activities to promote public confidence in the use of health IT and the exchange of EHI. These exceptions are intended to protect patient safety, promote the privacy of EHI, and promote the security of EHI.

The next three exceptions address activities to promote competition and consumer welfare. These exceptions would allow for the recovery of costs reasonably incurred, excuse an actor from responding to requests that are infeasible, and permit the licensing of interoperability elements on reasonable and non-discriminatory terms.

The last exception addresses activities that promote the performance of health IT; it recognizes that actors may make health IT temporarily unavailable for maintenance or improvements that benefit the overall performance and usability of health IT.

Pursuant to proposed §171.200, for any of the exceptions to the information blocking rule to apply, an actor must comply with all applicable terms and conditions of the exception(s) at all relevant times. The actor would have the burden of proof to demonstrate that compliance.

A. Exception — Preventing harm (§171.201)

ONC proposes an exception for reasonable and necessary practices to prevent harm to a patient or another person, subject to certain conditions which must be met at all relevant times. The conditions are as follows:

(1) *Types of Risks of Patient Harm.* The actor must have a reasonable belief that the practice will directly and substantially reduce the likelihood of harm to a patient or another person arising from—

- Corrupt or inaccurate data being recorded or incorporated in a patient's EHR;
- Misidentification of a patient or patient's EHI; or
- Disclosure of a patient's EHI in circumstances where a licensed health care professional has determined, in the exercise of professional judgment, that the disclosure is reasonably likely to endanger the life or physical safety of the patient or another person, provided that, if required by applicable federal or state law, the patient has been afforded any right of review of that determination.

ONC notes that the term patient does not necessarily require a clinician-patient relationship with the individual at risk of harm; health IT developers could benefit from this exception for individuals receiving care from a provider using the developer's health IT. The scope of the exception is limited to the risks specifically enumerated above. With respect to data corruption and inaccuracies, ONC clarifies that the recognized risk is limited to corruption and inaccuracies caused by performance and technical issues affecting health IT. For misidentification, ONC notes that the exception may apply to practices designed to promote data quality and integrity and support health IT applications properly identifying and matching patient records or EHI, which the agency notes is a complex task. Thus, where clinicians know a specific EHI in a patient's record is misattributed, it is reasonable for them not to share or incorporate that EHI. With respect to endangering life or physical safety, ONC envisions restrictions on disclosure of

an individual's EHI where a health care professional determines that disclosure is reasonably likely to pose a danger to the life or physical safety of the patient or another person.

To qualify for the exception, the actor must have a reasonable belief that the practice will directly and substantially reduce the likelihood of harm to a patient or another person. ONC proposes two methods to meet this condition: through a qualifying organizational policy or through a qualified individual finding.

(2) *Requirements for qualified organizational policies.* If the practice implements an organizational policy, it must be—

- In writing;
- Based on relevant clinical, technical, and other appropriate expertise;
- Implemented in a consistent and non-discriminatory manner; and
- No broader than necessary to mitigate the risk of harm.

For the practice to meet the third condition above (i.e., consistent and non-discriminatory implementation), ONC believes the actor should take reasonable steps to educate its directors, officers, employees, contractors, and authorized personnel on how to apply the policy and to provide appropriate oversight to ensure that the policy is not applied in an arbitrary, discriminatory, or otherwise inappropriate manner. For the fourth condition (i.e., narrowing the scope of the practice), ONC believes the policy should identify the relevant risks and mitigate those risks based on current patient safety evidence and best practices, supplemented by input from clinical, technical, and other staff.

(3) *Requirements for qualified individual finding*s. If the practice does not implement an organizational policy, an actor must make a finding in each case, based on the particularized facts and circumstances, and based on, as applicable, relevant clinical, technical, and other appropriate expertise, that the practice is necessary and no broader than necessary to mitigate the risk of harm. ONC proposes that health care professional's independent and individualized judgment about the safety of the actor's patients or other persons would be entitled to substantial deference, taking into account all relevant facts under the particular circumstances.

B. Exception — Promoting the privacy of electronic health information (§171.202)

ONC proposes an exception to protect the privacy of an individual's EHI. Under this exception, ONC identifies four methods, each with its own terms and conditions, by which the practice of an actor may qualify for protection under this exception to protect the privacy of an individual's EHI. ONC refers to these four methods as "sub-exceptions;" as is the case for each exception proposed under the rule, the terms and conditions of each "sub-exception" must be met at all relevant times. ONC notes that any privacy protection practice must be consistent with applicable laws related to health information privacy, such as the HIPAA Privacy Rule, the HITECH Act, 42 CFR Part 2, and state privacy laws.

ONC believes its privacy exception does not conflict with the HIPAA Privacy Rule framework and that it does promote patient privacy rights. However, ONC acknowledges that its information blocking rule may require actors to provide access, exchange, or use EHI in situations where HIPAA does not. HIPAA permits covered entities to use and disclose ePHI; the information blocking rule requires actors to provide access, to exchange, or to use EHI unless they are prohibited from doing so under federal or state law or are covered by one of the proposed exceptions.

Definition of individual. For purposes only of this exception and its four "sub-exceptions," ONC proposes to define "individual" in a more expansive manner than the term is defined under the HIPAA Privacy Rule or in section 3022 of the PHS Act. ONC proposes to define individual as meaning one or more of the following:

(1) An individual (as defined under the HIPAA Privacy Rule).
(2) Any other natural person who is the subject of the EHI being accessed, exchanged, or used.
(3) In relation to an individual described in (1) or (2) above:
    (i) A person who legally acts on behalf of such person, including as a personal representative, in accordance with the HIPAA Privacy Rule;
    (ii) A person who is a legal representative of and can make health care decisions on behalf of such person; or
    (iii) An executor, administrator or other person having authority to act on behalf of a deceased person or the individual's estate under state or other law.

ONC clarifies that the reason to include "any other natural person who is the subject of the EHI being accessed, exchanged, or used" in paragraph (2) above is to include EHI that would be accessed, exchanged, or used by entities that are not subject to HIPAA (i.e., entities that are not covered entities or business associates). The purpose of the proposed expansive definition is to protect information about all individuals, not just individuals whose EHI is protected as ePHI by HIPAA covered entities and business associates.

(1) *Sub-exception: Precondition imposed by law not satisfied.* Because state and federal privacy laws may impose conditions before disclosure of PHI is permitted, ONC proposes to protect actors who do not provide access, exchange or use EHI because a necessary precondition imposed under law for that disclosure has not been met. Thus, an actor in this situation may elect not to provide access, exchange, or use such EHI if the precondition under law has not been satisfied, subject to a number of conditions. However, ONC is concerned that an actor could use protection of an individual's privacy as a pretext for information blocking.

An actor could qualify for this exception by written organizational policies that specify the criteria an actor will use, and the steps the actor will take, to satisfy the legal precondition. This could include taking reasonable steps to ensure that the actor's workforce and its agents understand and consistently apply and actually follow the policies and procedures.

Alternatively, an actor could document, on a case-by-case basis, the criteria it uses to determine when the legal precondition would be satisfied, any criteria that were not met, and the reason why the criteria were not met. The documentation would have to identify the specific

circumstances of the practice, the criteria the actor used to determine that the precondition was satisfied, and the objective criteria the actor applied that are directly relevant to meeting the precondition.

Additionally, if the legal precondition relies on consent or authorization from an individual, the actor would have to do all things reasonably necessary within its control to provide the individual with a meaningful opportunity to provide the consent or authorization. This might mean a legally compliant consent form; ONC notes that a best practice would include informing the individual of the right to revoke consent. ONC cautions that the actor could not improperly encourage the individual to refuse to provide the consent or authorization.

ONC would also require that the actor's practice be tailored to the specific privacy risk or interest being addressed. ONC believes this would require the actor to carefully evaluate the privacy requirements imposed on the actor and the privacy interests to be managed by the actor, and to develop a considered response tailored to protecting and promoting the privacy of EHI.

Finally, the actor's practice must be implemented in a consistent and non-discriminatory manner; this means that the actor's privacy-protective practices must be based on objective criteria that apply uniformly for all substantially similar privacy risks.

(2) *Sub-exception: Health IT developer of certified health IT not covered by HIPAA*. Noting that the vast majority of developers of certified health IT are regulated by the HIPAA Privacy Rule because they operate as business associates to health care providers or plans and thus may use the first sub-exception described above, ONC notes that some direct-to-consumer products and services would not benefit from that sub-exception. For these developers of certified health IT not required to comply with the HIPAA Privacy Rule (referred to by ONC in this sub-exception as non-covered actors), ONC proposes to create this sub-exception. Non-covered actors who engage in a practice that promotes the privacy interests of an individual may choose not to provide access, exchange, or use of EHI if the practice meets all the following conditions:

- The practice complies with applicable state or federal privacy laws.
- The practice implements a process described in the actor's organizational privacy policy. ONC clarifies it expects detailed documentation of the processes and procedures used to determine when the actor will not provide access, exchange or use of EHI as well as a description of the specific requirements imposed on individuals giving consent.
- The practice had previously been meaningfully disclosed to the persons and entities that use the actor's product or service. In evaluating whether the disclosure is meaningful, ONC will consider whether the disclosure was in plain language and conspicuous. However, ONC notes non-covered actors would not have to disclose organizational privacy policy to its customers or to the public generally; rather, only the privacy-protective practices it has adopted must be described in sufficient detail.
- The practice is tailored to the specific privacy risk or interest being addressed.
- The practice is implemented in a consistent and non-discriminatory manner.

(3) S*ub-exception: Denial of an individual's request for their ePHI in the circumstances provided in 45 CFR 164.524(a)(1), (2), and (3).* Under the HIPAA Privacy Rule, covered entities (and in some instances business associates) may deny an individual access to PHI. the Privacy Rule establishes grounds for denial of access to PHI that are reviewable and other grounds for denial that are unreviewable. This exception would apply to both the unreviewable grounds and reviewable grounds of denials of access.

Unreviewable grounds. The unreviewable grounds for denial for individuals include situations involving the following:

- Certain requests made by inmates of correctional institutions;
- Information created or obtained during research that includes treatment, if certain conditions are met;
- Denials permitted by the Privacy Act; and
- Information obtained from non-health care providers pursuant to promises of confidentiality.

Additionally, two categories of information are expressly excluded from the individual right of access: psychotherapy notes[16] and information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

Reviewable grounds. The reviewable grounds of denial of access to PHI permit a covered entity to deny access if the individual is given a right to have that denial reviewed under certain circumstances. For example, a licensed health care professional, in the exercise of professional judgment, may determine that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person. If access is denied, then the individual has the right to have the denial reviewed by a licensed health professional who did not participate in the original decision to deny access.

ONC proposes a limited exception to permit a covered entity or business associate to deny an individual's request for access to their PHI on the basis of these unreviewable and reviewable grounds as long as the denial complies with HIPAA Privacy Rule requirements.

(4) *Sub-exception: Respecting an individual's request not to share information.* ONC believes an exception is necessary to ensure actors are confident that they may respect an individual's privacy choices when that individual specifically asks an actor not to provide access, exchange, or use EHI. Thus, ONC proposes that unless otherwise required by law, an actor may choose not to provide that access, exchange, or use if all of the following conditions are met:

- The individual requests the actor not to provide such access, exchange, or use.
- The individual initiates the request without any improper encouragement or inducement by the actor.
- The actor or its agent documents the request within a reasonable time period.
- The actor's practice is implemented in a consistent and non-discriminatory manner.

[16] Psychotherapy notes are the personal notes of a mental health care provider documenting or analyzing the contents of a counseling session that are maintained separate from the rest of the patient's medical record (see 45 CFR 164.524(a)(1)).

ONC notes that once a proper request is made, there would be no need for the individual to reiterate that request or for the actor to repeatedly reconfirm or re-document the request. ONC clarifies that individuals have the right to revoke a request not to share information.

C. Exception — Promoting the security of electronic health information (§171.203)

Noting that actors may be reluctant to implement security measures or otherwise safeguard the confidentiality, integrity and availability of EHI without an exception to the information blocking rule, ONC proposes an exception to permit actors to engage in reasonable and necessary practices to promote the security of EHI. ONC is concerned that the information blocking rule could discourage best practice security protocols and diminish the reliability of the health IT ecosystem. However, ONC is also concerned about practices purporting to promote the security of EHI but that may be unreasonably broad, onerous on those seeking access to the EHI, not applied consistently across/within an organization, or otherwise unreasonably interfere with access, exchange, or use of EHI. ONC also notes that a practice that complies with the HIPAA Security Rule might not necessarily qualify for this proposed exception.

(1) *Conditions.* To qualify for this exception, each practice by an actor must meet all the following conditions:

- The practice must be directly related to safeguarding the confidentiality, integrity, and availability of EHI. ONC would examine whether the practice directly addresses specific security risks (and whether it served other purposes) to determine the necessity of the practice and its direct relation to safeguarding EHI.
- The practice must be tailored to the specific security risk being addressed. ONC expects actors to have carefully evaluated the security risk and developed a considered response tailored to mitigating the specific vulnerability.
- The practice must be implemented in a consistent and non-discriminatory manner.

Actors could meet the requirements for this exception through practices that implement either security policies and practices developed by the actor (i.e., organizational security policies) or through case-by-case determinations.

(2) *Organizational security policies.* If the practice implements an organizational security policy, the policy must—

- Be in writing;
- Be prepared on the basis of, and directly respond to, security risks identified and assessed by or on behalf of the actor;
- Align with one or more applicable consensus-based standards or best practice guidance; and
- Provide objective timeframes and other parameters for identifying, responding to, and addressing security incidents.

To support a presumption that an actor's security policy is reasonable, ONC believes the policy must be informed by an assessment of the security risk (e.g., threat and vulnerability analysis, data collection, security measures, etc.); must align with one or more applicable consensus-based standards; and must provide objective timeframes and common terminology to identify, respond to, and address security incidents. ONC notes that compliance with the HIPAA Security Rule is relevant but not dispositive to the issue of whether the policy is objectively reasonable. ONC believes documented policies should include specific references to consensus-based standards and best practice guidance.

(3) *Case-by-case determinations.* While ONC expects most security practices will implement organizational security policies, there may be occasions when novel and unexpected threats require action to mitigate a security risk. Thus, where a practice does not implement an organizational security policy, to qualify for this exception an actor must determine in each case, based on the particularized facts and circumstances, that—

- The practice is necessary to mitigate the security risk to EHI; and
- There are no reasonable and appropriate alternatives to the practice that address the security risk that are less likely to interfere with, prevent, or materially discourage access, exchange or use of EHI.

ONC notes that what constitutes reasonable and appropriate alternatives will depend on the urgency and nature of the specific security threat.

D. Exception — Recovering costs reasonably incurred (§171.204)

ONC proposes an exception to permit actors to recover certain costs they reasonably incur in providing access to, exchange of, or use of EHI that would promote innovation, competition, and consumer welfare. This is necessary because ONC interprets the definition of information blocking to include any fee likely to interfere with access, exchange or use of EHI. ONC believes that absent an exception, actors may be unable to recover costs they incur to develop technologies and provide services that enhance interoperability. To qualify for this exception, each practice by an actor must meet all the following conditions. ONC is concerned by rent-seeking, opportunistic fees, and exclusionary practices that interfere with access, exchange and use of EHI as well as by discriminatory pricing policies that exclude competitors from use of interoperability elements. ONC emphasizes that all the conditions would have to be satisfied for each and every fee charged by an actor.

(1) *Types of costs*. ONC would tailor the exception to the actor's costs reasonably incurred to provide access, exchange, or use of EHI. While noting that this is a factual determination, ONC states these would not include speculative or subjective costs. Further, ONC says that the exception would not apply to fees (e.g., those based on profit or revenue for use of EHI) that exceed the actor's reasonable costs for providing access, exchange or use of EHI.

(2) *Method for recovering costs*. The method by which the actor recovers its costs would have to be reasonable and non-discriminatory. Specifically, the method for recovering costs must meet all the following conditions:

- It must be based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests.
- It must be reasonably related to the actor's costs of providing the type of access, exchange, or use to the person or entity to whom the fee is charged. ONC clarifies that an actor is not required to apply the same prices or price terms for everyone to whom it provides services; however, any price differences would have to be based on actual differences in costs the actor incurred or on other reasonable or non-discriminatory criteria.
- It must be reasonably allocated among all customers to whom the technology or service is supplied, or for whom the technology is supported. ONC notes that an actor must allocate costs using reasonable criteria and allocate them among customers that caused the costs to be incurred or that benefit from the technology. ONC also cautions that actors may not recover all core costs from each customer.
- It must not be based in any part on whether the requestor or other person is a competitor, potential competitor, or will be using the EHI in a way that facilitates competition with the actor.
- It must not be based on the sales, profit, revenue, or other value that the requestor or other persons derive or may derive from the access, exchange, 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 revenue-sharing or profit-sharing arrangements would only be covered by the exception if they are designed to provide an alternative way to recover costs reasonably incurred for providing the services.

(3) *Costs specifically excluded*. ONC excludes certain types of costs from protection under this exception to the information blocking rule. Specifically, the exception would not apply to any of the following costs or fees:

- Costs due to non-standard design or implementation choices. These are costs actors incur because the health IT is designed or implemented in non-standard ways that unnecessarily increase the complexity, difficulty or burden of accessing, exchanging, or using EHI.
- Subjective or speculative costs. These are costs associated with intangible assets (including depreciation or loss of value), other than the actual development or acquisition costs of such assets, or opportunity costs, except for the reasonable forward-looking cost of capital.
- The types of fee that covered entities may not impose under the HIPAA Privacy Rule for requests by an individual for a copy of PHI. Examples of these prohibited costs include costs associated with verification; documentation; searching for and retrieving the PHI; maintaining systems; and recouping capital for data access, storage, or infrastructure.[17]
- A fee based in any part on the electronic access by an individual or their personal representative, agent, or designee to the individual's EHI. ONC distinguishes these fees from cost-based fees that a covered entity may charge individuals for copies of ePHI under HIPAA and similar allowable costs under state laws and which may be excluded under this exception.

[17] See 45 CFR 164.524(c)(4): https://www.ecfr.gov/cgi-bin/text-idx?SID=7a76846e7aa7284ba0e5cb99dcdea8c4&mc=true&node=se45.1.164_1524&rgn=div8.

- A fee to perform an export of EHI via the capability of health IT certified to the EHI certification criterion[18] to switch health IT or to provide patients their EHI.
- A fee to export or convert data from an EHR technology, unless such fee was agreed to in writing at the time the technology was acquired.

ONC also clarifies that access to EHI that is provided by physical media (e.g., paper copies, or where EHI is copied onto a CD or flash-drive) would not be a practice that implicates the information blocking rule as long as the fee charged for that access complied with the HIPAA Privacy Rule. ONC believes the last two examples of costs specifically excluded from this exception (those relating to export and portability of EHI in EHR systems) are the types of costs specifically contemplated by the information blocking rule. ONC notes that providers often encounter rent-seeking and opportunistic pricing practices when they export EHI from their systems for use with other technologies that compete with or reduce revenue opportunities with an EHR developer's own products and services.

However, ONC clarifies that a developer could still charge a fee to deploy EHI export capabilities in a health care provider's production environment or to provide additional services on top of those reasonably necessary to enable its intended use. Additionally, because the EHI certification criterion provides only a baseline capability for exporting data, developers of certified health IT may need to provide other data portability services to facilitate the smooth transition of data from health care providers between different health IT systems; fees for those services may qualify for protection under the exception if they meet the conditions for this exception as well as the exception for requests that are infeasible under the exception proposed at
§171.205 (described below). These fees would have to be agreed to in writing when the technology is acquired.

(4) *Compliance with the Conditions of Certification*. ONC notes that a health IT developer of certified health IT subject to the API Condition of Certification[19] may not charge certain types of fees and also are subject to more specific cost accountability rules than apply under this proposed exception. ONC proposes that the developer must comply with all requirements of such conditions of certifications for all practices and at all relevant times to qualify for this exception from the information blocking rule. Additionally, ONC proposes that an API Data Provider (including a health care provider that acts as an API Data Provider) may only charge the same fees that an API Technology Supplier may charge to recover costs consistent with the permitted fees specified in the API Condition of Certification.

E. Exception — Responding to requests that are infeasible (§171.205)

As noted earlier, the information blocking rule would be implicated if an actor refuses to facilitate access, exchange, or use of EHI, either as a general practice or in isolated instances. However, ONC notes that in certain circumstances there are legitimate practical challenges beyond an actor's control which limit its ability to comply with requests for that access,

[18] See 45 CFR 170.315(b)(10) in the ONC proposed rule.
[19] See 45 CFR 170.404 in the ONC proposed rule, which is summarized in Appendix A to this HPA summary.

exchange, or use either because the actor may not have (or may be unable to obtain) the necessary technological capabilities, legal rights, financial resources, or other means necessary to provide a particular form of access, exchange, or use or because the actor would incur costs or other burdens that are clearly unreasonable under the circumstances. ONC proposes an exception that would permit an actor to decline a request when carrying out the request would be infeasible or impossible and when the actor otherwise did all that it reasonably could under the circumstances to facilitate other means of accessing, exchanging, and using the EHI. ONC would use a structured, fact-based approach for determining whether a request was infeasible, focusing on the immediate and direct financial and operational challenges of facilitating access, exchange, or use rather than remote, indirect, or speculative types of harm.

(1) *Request is infeasible*. ONC proposes a two-step test to determine when a request is infeasible: the actor must demonstrate that the request poses a substantial burden and that assuming that burden is plainly unreasonable under the circumstances.

Substantial burden. The actor must demonstrate that complying with the request in the manner requested would impose a substantial burden on the actor. ONC believes that actors would most likely meet this requirement by showing that they did not have, and could not readily obtain, the requisite technological capabilities, legal rights, or other means necessary to facilitate the particular type of access, exchange, or use requested. Actors could also show that complying with the request would have caused a significant disruption to its health care or business activities or that it would have incurred significant unbudgeted costs.

In determining whether a burden is substantial for this test, ONC would take a fact-specific approach and consider an actor's particular circumstances, including the type of actor, the nature and purpose of its business or other activities, and the financial, technical, and other resources and expertise at its disposal. It would also consider any possible offsetting benefits of complying with the request, such as meeting statutory or regulatory requirements.

Plainly unreasonable. ONC proposes a number of factors it would consider to determine whether a substantial burden is plainly unreasonable under the circumstances:

- The type of EHI and the purposes for which it may be needed;
- The cost to the actor of complying with the request in the manner requested;
- The financial, technical, and other resources available to the actor;
- Whether the actor provides comparable access, exchange, or use to itself or to its customers, suppliers, partners, and other persons with whom it has a business relationship;
- Whether the actor owns or has control over a predominant technology, platform, health information exchange, or health information network through which EHI is accessed or exchanged;
- Whether the actor maintains ePHI on behalf of a HIPAA covered entity or maintains EHI on behalf of the requestor or another person whose access, exchange, or use of EHI will be enabled or facilitated by the actor's compliance with the request;
- Whether the requestor and other relevant persons can reasonably access, exchange, or use the EHI from other sources or through other means; and

- The additional cost and burden to the requestor and other relevant persons of relying on alternative means of access, exchange, or use.

ONC would consider the type of EHI at issue, the purposes for which the EHI is needed, the severity of the burden imposed on the actor, and the frequency of the type of request at issue. ONC would balance the burdens against the costs to the requestors (and other persons) who would be harmed by the refusal to provide the access, exchange or use, including whether the requestor could have acquired the EHI through other means. Finally, ONC would also consider the balancing of relative burdens in conjunction with the actor's control over interoperability elements; for example, a dominant health system that provides local health IT infrastructure would have to demonstrate an extreme hardship to justify denying interconnection requests or access to interoperability elements.

ONC notes that an actor could be covered under this exception if it is unable to provide access, exchange or use of EHI due to a natural disaster (e.g., hurricane or earthquake) or war.

Plainly not burdensome. ONC indicates that the following circumstances do not constitute a burden to the actor for purposes of this exception; ONC would not consider them in determining whether a request is infeasible.

- Providing the requested access, exchange, or use in the manner requested would have facilitated competition with the actor.
- Providing the requested access, exchange, or use in the manner requested would have prevented the actor from charging a fee.

(2) *Responding to requests*. The actor would have to respond to all requests relating to access, exchange, or use of EHI in a timely manner, including requests to establish connections and to provide interoperability elements. ONC would analyze whether a response is timely based on what is objectively reasonable for the actor.

(3) *Written explanation*. The actor would have to provide the requestor with a detailed written explanation of the reasons why the actor cannot accommodate the request.

(4) *Provision of a reasonable alternative*. The actor must work with the requestor in a timely manner to identify and provide a reasonable alternative means of accessing, exchanging, or using the EHI.

F. Exception — Licensing of interoperability elements on reasonable and nondiscriminatory terms (§171.206)

ONC states that the information blocking rule would be implicated if an actor refuses to license or allow the disclosure of interoperability elements to persons who require those elements to develop and provide interoperable technologies or services (including those that might complement or compete with the actor's own technology or services), or if the actor licensed interoperability elements subject to terms or conditions that have the purpose or effect of excluding or discouraging competitors, rivals, or other persons from engaging in pro-competitive

and interoperability enhancing activities. The preamble includes examples of situations that do and do not implicate the information blocking rule. ONC is concerned by the use of contractual and intellectual property rights to extract rents for access to EHI or to prevent competition from developers of interoperable technologies which it believes undermines the fundamental objectives of the information blocking rule.

ONC proposes to establish an exception to permit actors to license interoperability elements on reasonable and non-discriminatory (RAND) terms, subject to certain strict conditions to ensure that actors license interoperability elements on those terms and that they do not impose collateral terms or otherwise impede use of interoperability elements. Acknowledging that its proposal to prevent intellectual property owners from extracting rents for access to EHI differs from standard intellectual property policy, ONC believes its proposal to limit rents to RAND terms is essential because rents will likely frustrate access, exchange and use of EHI. ONC notes that actors who do not want to license a particular technology may choose to develop and provide alternative means to access, exchange and use EHI as long as it is similarly efficient and efficacious. To qualify for this exception, each practice by an actor would have to meet the following conditions at all relevant times.

(1) *Reasonable and non-discriminatory (RAND) terms*. To qualify for this exception, actors must license interoperability elements on terms that are reasonable and nondiscriminatory. ONC notes that standards development organizations have policies requiring members who contribute technologies to a standard to voluntarily commit to license those technologies on RAND terms. ONC believes its proposed RAND requirement balances the need for robust intellectual property (IP) protections with the need to ensure that this proposed exception does not permit actors to exercise their IP or other proprietary rights in inappropriate ways that block the development, adoption, or use of interoperable technologies and services. To meet the RAND condition, actors must comply with the following requirements:

Responding to requests. Upon receiving a request to license or use interoperability elements, the actor must respond to the requestor within 10 business days from receipt of the request. That response would require negotiating with the requestor in a reasonable and non-discriminatory fashion to identify the interoperability elements that are needed and offering an appropriate license with reasonable and non-discriminatory terms. ONC notes that actors are not required to grant a license in all instances as long as the negotiations are conducted under RAND terms and an offer pursuant to those negotiations is made. ONC does not propose to establish a deadline by which negotiations must be concluded.

Scope of rights. ONC proposes that an actor must license the requested interoperability elements with all rights necessary for access and use for the following purposes, as applicable:

- Developing products or services that are interoperable with the actor's health IT, health IT under the actor's control, or any third party who currently uses the actor's interoperability elements to interoperate with the actor's health IT or health IT under the actor's control. ONC notes this would include the right to incorporate and use the interoperability elements in the licensee's own technology to the extent necessary.

- Marketing, offering, and distributing the interoperable products and/or services to potential customers and users. This would include the right to copy or disclose the interoperability elements as necessary.
- Enabling the use of the interoperable products or services in production environments, including accessing and enabling the exchange and use of EHI.

Reasonable royalty. If the actor charges a royalty for the use of interoperability elements, the royalty would have to be reasonable. To qualify for this exception, a royalty would have to meet the following requirements:

- The royalty must be non-discriminatory.
- The royalty must be based solely on the independent value of the actor's technology to the licensee's products, not on any strategic value stemming from the actor's control over essential means of accessing, exchanging, or using EHI.
- If the actor has licensed the interoperability element through a standards development organization in accordance with such organization's policies regarding the licensing of standards-essential technologies on RAND terms, the actor may charge a royalty that is consistent with those policies.

ONC lists 10 factors that it may consider in determining whether a royalty is reasonable which the agency says mirror factors used by courts considering the reasonableness of royalties charged under a commitment to a standards development organization to license technologies on RAND terms.

Non-discriminatory terms. ONC would require that the terms on which an actor licenses and otherwise provides the interoperability elements must be non-discriminatory; this would apply to terms that relate to the price as well as other terms such as royalties. The actor would have to comply with the following requirements:

- The terms must be based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests.
- The terms must not be based in any part on—
    - Whether the requestor or other person is a competitor, potential competitor, or will be using EHI obtained via the interoperability elements in a way that facilitates competition with the actor; or
    - The revenue or other value the requestor may derive from access, exchange, or use of EHI obtained via the interoperability elements, including the secondary use of the EHI.

ONC notes that actors do not have to apply the same terms for all persons requesting a license, but differences in terms must be based on actual, legitimate differences in costs the actor incurs or on other non-discriminatory criteria that are objectively verifiable. For example, an actor could provide more favorable terms under a joint venture or co-marketing agreement than it might provide under arms-length transactions. However, ONC reminds developers of certified health IT that the Condition of Certification under proposed §170.404 would preclude the developer from offering APIs on different terms.

Collateral terms. ONC proposes 5 additional conditions that it says would provide "bright-line prohibitions" for certain types of collateral terms or agreements that it believes will interfere with access, exchange, or use of EHI. To qualify for this exception, ONC proposes to prohibit an actor from requiring a licensee or its agents or contractors to do, or to agree to do, any of the following:

- Not compete with the actor in any product, service, or market.
- Deal exclusively with the actor in any product, service, or market.
- Obtain additional licenses, products, or services that are not related to or can be unbundled from the requested interoperability elements. ONC is concerned that actors could require licensees to take license to interoperability elements it does not want; this would permit the actor to extract royalties inconsistent with the requirement for RAND terms and conditions. However, nothing would preclude an actor and licensee from voluntarily agreeing to such an arrangement.
- License, grant, assign, or transfer to the actor any intellectual property of the licensee. However, a willing agreement between the parties to cross-license or co-market intellectual property would be permissible.
- Pay a fee of any kind (other than a reasonable royalty described above) unless the practice meets the requirements of the proposed exception for costs reasonably incurred at §171.204 (described above).

Non-disclosure agreement. ONC proposes to allow an actor to require a reasonable non-disclosure agreement that is no broader than necessary to prevent unauthorized disclosure of the actor's trade secrets. The agreement would have to specify all information the actor claims as trade secrets, and the information would have to meet the definition of a trade secret under applicable law. ONC notes that a developer of certified health IT may be subject to the Condition of Certification proposed in the ONC proposed rule at §170.403 (which prohibits certain health IT developer prohibitions and restrictions on communications about the developer's technology and business practices), and if so, this exception would not affect the developer's obligations to comply with that condition.

(2) *Additional requirements relating to the provision of interoperability elements*. To qualify for this exception, an actor could also not engage in any practice that has any of the following purposes or effects:

- Impeding the efficient use of the interoperability elements to access, exchange, or use EHI for any permissible purpose.
- Impeding the efficient development, distribution, deployment, or use of an interoperable product or service for which there is actual or potential demand.
- Degrading the performance or interoperability of the licensee's products or services, unless necessary to improve the actor's technology and after affording the licensee a reasonable opportunity to update its technology to maintain interoperability.

ONC says the intent behind these additional conditions is to ensure that actors who license interoperability elements on RAND terms do not engage in separate practices that impede the use of those interoperability elements or otherwise undermine the intent of this exception. ONC

notes these additional conditions address a broader range of practices that may not be effected through license agreements or that occur outside licensing negotiations. ONC does clarify that this condition would not prevent an actor from making improvements to its technology or responding to its customers' or users' needs; however, the actor's practice would need to be necessary to accomplish these purposes, and the actor must provide the licensee a reasonable opportunity to update its technology to maintain interoperability.

(3) *Compliance with conditions of certification*. ONC notes that a health IT developer subject to the conditions of certification proposed in the ONC rule at §§170.402, 170.403, or 170.404 must comply with all requirements of such conditions for all practices and at all relevant times.

G. Exception — Maintaining and improving health IT performance (§171.207)

Noting that health IT needs to be maintained and occasionally improved, and that performing maintenance or improvement requires the health IT to be temporarily taken offline, ONC proposes an exception to the information blocking rule for practices that are reasonable and necessary to maintain and improve the overall performance of health IT, subject to certain conditions. This exception would apply to both planned and unplanned maintenance and improvement. ONC acknowledges that health IT performance is often measured by service level agreements that provide flexibility to ensure that system availability is balanced with essential maintenance and improvements. Where the provision of health IT is subject to an allowance for maintenance or improvement that has been agreed to by the recipient of that health IT, ONC proposes that neither that agreement, nor the performance of it, should constitute information blocking, provided that certain conditions are met.

(1) *Maintenance and improvements to health IT*. An actor may make health IT under its control temporarily unavailable in order to perform maintenance or improvements to the health IT if the actor's practice is—

- For a period of time no longer than necessary to achieve the maintenance or improvements;
- Implemented in a consistent and non-discriminatory manner; and
- If the unavailability is initiated by an actor that is a health IT developer of certified health IT, a HIE, or a HIN, the practice is agreed to by the individual or entity to whom the actor supplied the health IT.

ONC notes that it would be more difficult to evaluate what time period is "no longer than necessary" in the case of unplanned maintenance or improvement since these are typically initiated by a threat or risk that must be responded to urgently and for as long as the risk persists. With respect to agreements with recipients of health IT, ONC notes that availability of health IT is typically addressed in contracts or other agreements which puts recipients on notice about the level of unavailability (both planned and unplanned) that may be expected. For situations where health IT must be taken offline on an urgent basis that is not expressly permitted in a contract, ONC notes the actor could still satisfy this condition by providing oral notice to the recipient.

ONC also notes that when a recipient or customer (as opposed to the supplier of health IT) initiates unavailability, no agreement is necessary for the customer (e.g., a health care provider)

to benefit from this exception. However, unavailability initiated by a recipient or customer would still need to satisfy the other conditions of this exception.

(2) *Practices that prevent harm*. If the unavailability of health IT for maintenance or improvements is initiated by an actor in response to a risk of harm to a patient or another person, the actor would not need to satisfy the requirements of this exception; however, the actor would have to comply with all the requirements for the exception for preventing harm proposed at §171.201 (described above) at all relevant times to qualify for an exception.

(3) *Security-related practices*. If the unavailability of health IT for maintenance or improvements is initiated by an actor in response to a security risk to EHI, the actor would not need to satisfy the requirements of this exception; however, the actor would have to comply with all requirements for the exception for promoting the security of EHI proposed at §171.203 (described above) at all relevant times to qualify for an exception.

ONC is considering whether to expand this exception to include a broader class of practices that are the subject of reasonable commercial agreements that may be considered information blocking absent an exception, such as "throttling" or "metering" availability of health IT.

III. Additional Exceptions—Request for Information

ONC is considering whether it should propose in future rulemaking a narrow exception to the information blocking rule for practices that are necessary to comply with the requirements of the Common Agreement. This would be intended to support adoption of the Common Agreement and encourage other entities to participate in trusted exchange. The exception would provide protection for practices expressly required by the Common Agreement or necessary to implement those requirements. ONC expects that its proposed exception would apply only to contract terms, policies and other practices that are strictly necessary to comply with the Common Agreement, and the exception would apply to practices that are no broader than necessary under the circumstances.

ONC seeks feedback on this potential exception, including whether it is necessary and whether there could be negative effects.

Separately, ONC welcomes comment on potential additional exceptions it should consider for future rulemaking.

IV. Complaint Process

Section 3022 of the PHS Act requires ONC to implement a standardized process for the public to submit reports on claims of health information blocking and that collects certain information, such as the originating institution, location, type of transaction, system and version, timestamp, terminating institution, locations, system and version, failure notice, and other related information.

ONC indicates that it will implement the process by building on existing mechanisms, including the current complaint process at https://www.healthit.gov/healthit-feedback. **ONC seeks comment on this approach as well as on the following specific issues:**

- What types of information are most important to collect in order to identify potential instances of information blocking?
- What types of information are contemplated by the following categories: the originating institution; location; type of transaction; system and version; timestamp; terminating institution; locations; system and version; failure notice; and other related information?
- What types of information or data elements should be collected under each of the above categories?
- What additional types of information beyond the above may be relevant to complaints and allegations of information blocking, especially practices that involve contractual or other business practices for which some of the categories of technical or transactional information above may not apply?
- How can ONC encourage and streamline the collection of such information so as to minimize burden and encourage the submission of complaints, especially complaints about practices that raise the types of information blocking concerns described in this proposed rule?
- How can ONC facilitate the inclusion of sufficient detail and granularity in complaints to enable effective investigations?
- What safeguards should be provided to support adequate confidentiality and handling of information that could: (1) identify the source of the complaint or allegation; (2) contain other individually identifiable information; and (3) contain confidential or proprietary business information?

V. Disincentives for Health Care Providers - Request for Information

Section 3022 of the PHS Act requires the application of "appropriate disincentives" under existing federal law for health care providers who violate the information blocking rule, and directs the Secretary to establish those disincentives through rulemaking. ONC is concerned that existing law may be insufficient to cover the range of conduct that could fall under the information blocking rule.

ONC seeks information on existing disincentives, as well as potential modifications to them, that would serve as effective deterrents. ONC also seeks information on avoiding duplicate penalty structures that would otherwise apply with respect to information blocking and the type of individual or entity involved before the date of enactment of the Cures Act.