Summary of the Office of the National Coordinator for Health IT's (ONC) 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Final Regulation

Table of Contents

I. Overview

On May 1, 2020 (effective date June 30, 2020), ONC published a final regulation aiming to improve patient access to data and electronic health information exchange, or interoperability. The ONC rule, known as the 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, is primarily focused on the health IT vendor community, including health IT vendors and health information exchanges and networks, as well as the physicians using those systems. ONC updated elements of their certification program and outlined requirements for vendors to use standards-based application programming interfaces (APIs) to exchange health data electronically. Another significant portion of ONC's rule – and the aspect that is directly related to actions physicians take – includes ONC's definition of what constitutes information blocking, clarifying the 21st Century Cures Act definition, and outlines the eight exceptions to information blocking.

II. Key Takeaways and Implications

a. ACP Supports

Advancing interoperability in stages: One of the more significant changes from proposed to final rule, and one of ACP's big asks, was taking efforts to improve data exchange in stages so that risks and benefits can be assessed appropriately before opening the floodgates for increased clinical data exchange.

- The key policy change was ONC scaling back their definition of electronic health information that physicians would be required to exchange upon request.
- The proposed definition was extremely broad and could have covered any piece of electronic data that existed on the patient.
- The final rule scaled that definition back to encompass electronic protected health information as defined by HIPAA, which aligns the definition with existing regulations as opposed to adding another definition or layer of complexity.
- Additionally, ONC is allowing a "first stage" of implementation – meaning that for the first 18 months (beginning six months after the publication of final rule), physicians will only be required to share a core set of accepted data elements (the US Core Data for Interoperability, USCDI) for the purposes of the information blocking provisions.

Promoting health IT standards and standards-based APIs: The College strongly supports ONC requiring the use of modern interoperability health IT standards (Fast Healthcare Interoperability Resources [FHIR]) and standards-based APIs. These technical requirements are an essential component in health information exchange and have the potential to greatly advance patients' access to their data and the exchange and use of information among physicians.

Requiring security specifications for electronic health data: ONC addressed security concerns through implementation specifications for oAuth 2.0 (but not privacy issues, as discussed below).

Promoting usability and safety of health IT: ONC finalized removal of gag clauses in vendor contracts allowing clinicians to share screenshots/videos regarding a number of usability and safety issues.

b. ACP'S Remaining Concerns

Privacy of electronic health data: ONC did not fully address the underlying privacy policy concerns regarding patient data and third-party apps accessing data through APIs; they are essentially leaving it to others in industry to layer privacy policies on top of the security specifications.

- Scaling back to focus on USCDI elements first and then expand to the existing ePHI definition provides some initial guardrails, which is a positive.
- Clinicians are essentially prohibited from vetting apps chosen by patients (and cannot reject an app due to privacy concerns). They are welcome to set up education program to explain concerns and provide guidance to patients.

Burden of Information Blocking Provisions – Implementation and Compliance: ONC provided further clarification and included an additional exception that seems to allow for a bit more flexibility for physicians – "Content and Manner Exception" – however, the exceptions still leave a lot of room for varying interpretation.

- The College remains concerned around the downstream, and likely burdensome, effects these provisions will have on day-to-day physician practice – each specific exception requires extensive documentation, and each exception is different.

Costs associated with implementing and maintaining APIs/data exchange services: Clinicians will have to pay to implement and operate functionality but cannot charge patients for these exchange services.

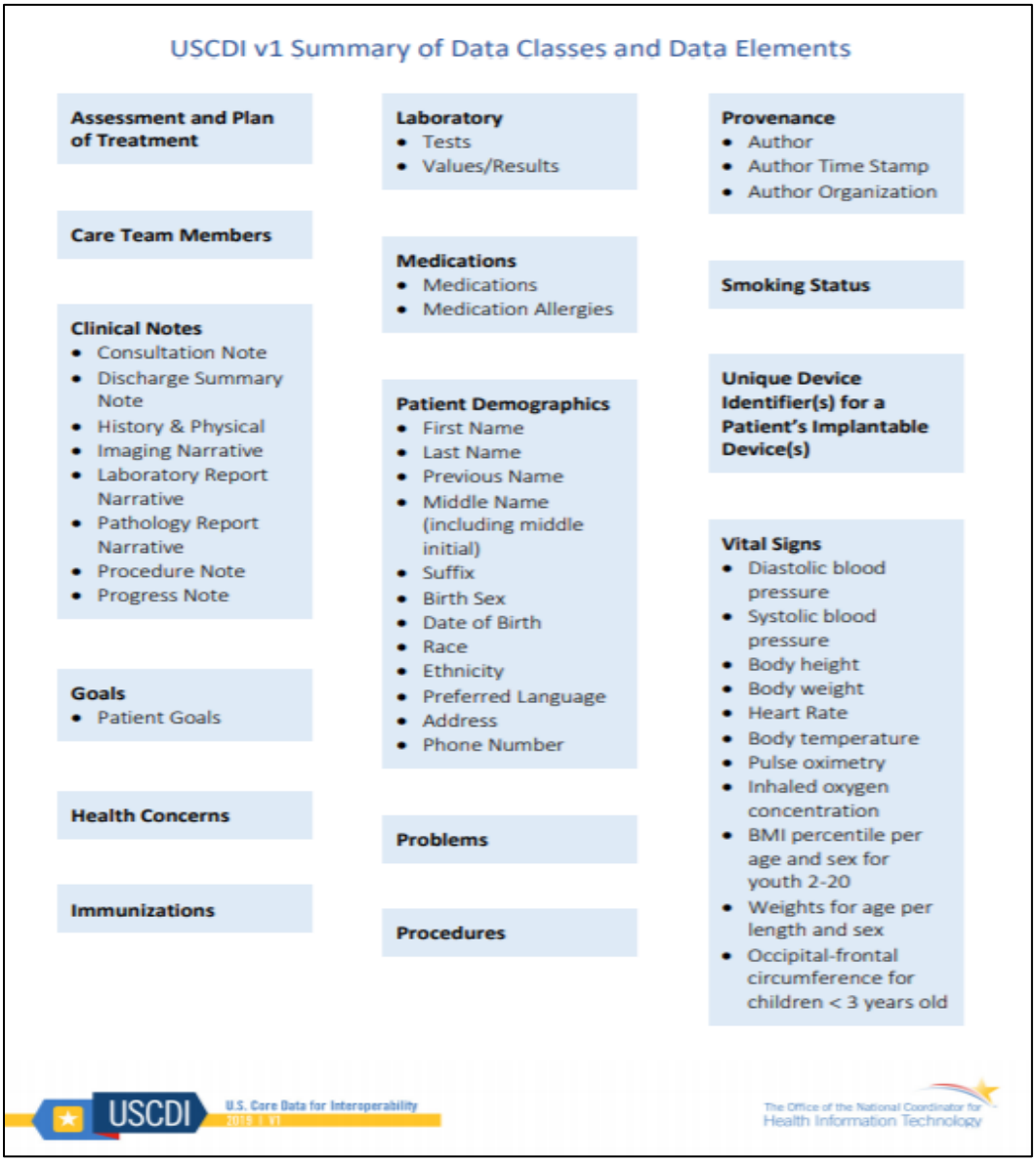
Development and Implementation Timelines: There are still a number of varying compliance and implementation deadlines, and we remain concerned about when the technical upgrades will be ready versus when physicians will be required to use the technology. There is no designated implementation window for physicians.

III. Summary of Key Provisions in ONC Final Rule

a. Updates to the 2015 Edition Certified Electronic Health Record Technology Criteria

United States Core Data for Interoperability (USCDI)

- Finalized first version of USCDI as a standard and replaces the Common Clinical Data Set (CCDS). USCDI is the minimum baseline of data classes (e.g., patient demographics) and data elements (e.g., patient name) that are available for interoperable exchange, and is designed to be expanded through an iterative process over time.
- Adoption and use of USCDI will advance interoperability by ensuring utilization of common data and vocabulary codes sets. This standardization will support both electronic exchange and usability of the data.



Source: https://www.healthit.gov/isa/sites/isa/files/2020-03/USCDI-Version1-2020-Final-Standard.pdf

Electronic Prescribing

- Adopted National Council for Prescription Drug Programs (NCPDP) SCRIPT standard for e-prescribing to align with CMS regulations.
- Additionally, ONC adopted the same electronic Prior Authorization (ePA) request and response transactions supported by the NCPDP SCRIPT standard proposed by CMS.

Clinical Quality Measures – Report

- Removed HL7 Quality Reporting Document Architecture (QRDA) standard requirements and instead requires Health IT Modules to support the CMS QRDA Implementation Guide, removing certification requirements that do not support quality reporting for CMS programs.

Electronic Health Information (EHI) Export

- Refined the scope of data a Health IT Module must export and aligned the criterion to the new definition of EHI.
- ONC does not require standards for the export format(s) used to support the export functionality – this could cause implementation and usability issues if there are a number of varying export formats.
- Consistent with the "Assurances" Condition of Certification, developers of certified health IT must provide such capabilities to their customers within 36 months of the final rule's publication date (compared to 24 months as proposed).

Application Programming Interfaces (APIs)

- Separate from "EHI Export" criterion:
    - The "EHI export" criterion focuses on a Health IT Module's ability to electronically export EHI that can be stored at the time of certification by the product, of which the Health IT Module is a part.
    - In contrast, the finalized API criterion focuses on "read" services for single and multiple patients for the USCDI Data Elements and US Core IG FHIR profiles.
    - As noted above, the "EHI export" criterion does not mandate conformance to standards or implementation specifications, whereas the API criterion requires conformance to several standards and implementation specifications.
- ONC adopted a new API certification criterion to replace the "application access – data category request" certification criterion:
    - The new "standardized API for patient and population services" certification criterion focuses on supporting two types of API-enabled services:
        - Services for which a single patient's data is the focus, and
        - Services for which multiple patients' data are the focus.
    - Uses HL7 FHIR standard Release 4.
- Vetting of third-party apps by clinicians accessing health IT system via API's (outside of the scope of the technical conformance requirements for certified health IT):
    - All other practices associated with third-party application review or "vetting" by implementers (clinicians) must not violate the information blocking provisions (described in more detail later).
    - In general, clinicians will be allowed to review third-party applications they intend to use for their own business (e.g., a third-party decision-support application used by the health care

provider in the course of furnishing care) prior to permitting the third-party applications to connect to their deployed APIs within its enterprise and clinical users' workflow.
    - However, clinicians are not permitted to review or "vet" third-party applications intended for patient access and use.
- API Fees:
    - ONC is promoting transparent documentation of all permitted fees to maintain a competitive marketplace and ensure that fees are reasonably related to the development, deployment, upgrade, and use of certified API technology.
    - ONC argues fee transparency also enables clinicians and patients to shop for certified API technology and related services that meet their needs.
    - The fee requirements under the Conditions of Certification only apply to API developers. Clinicians would generally be expected to recover these costs through fees administered while delivering health care services.
    - ONC disagrees that costs for updating information systems and Health IT Modules to the new standards and requirements would be passed on to physicians and patients.
        - Most of the information contained in a patient's electronic record has been documented during the practice of medicine or has otherwise been captured in the course of providing health care services to patients.
        - In their view, patients have effectively paid for this information, either directly or through their employers, health plans, and other entities that negotiate and purchase health care items and services on their behalf, and should be able to access the information via certified API technology and without fees.

Privacy and Security Transparency Attestations

- Adopted two new privacy and security criteria requiring transparency attestations from developers of certified health IT.
    - Will serve to identify whether or not certified health IT supports encrypting authentication credentials and/or multi-factor authentication.

Security Tags and Consent Management

- Updated requirements for "data segmentation for privacy" (DS4P) certification criteria to support security tagging at the document, section, and entry levels.

b. Modifications to the ONC Health IT Certification Program

Privacy and Security Certification Framework

- ONC finalized corrections to the 2015 Edition Privacy and Security Certification Framework.

Certification Companion Guides (CCGs)

- ONC finalized corrections to the 2015 Edition CCGs.

Principles of Proper Conduct (PoPC) for ONC-ACB's

- ONC adopted new and revised PoPCs for ONC-ACB's who are responsible for conducting ongoing surveillance activities to assess whether certified health IT meets certification requirements.

Certification of Complete EHRs and Health IT Modules

- ONC finalized clarification that the records retention provision includes "life of the Edition" as well as three years after the retirement of an Edition.

Additional Revisions to PoPC

- ONC finalized revisions to the PoPC to clarify the basis for certification, including to permit a certification decision be based on an evaluation conducted by the ONC-ACB by use of conformity methods approved by the National Coordinator.

Acceptance of Certification Test Results

- ONC finalized requirement for ONC-ACBs to accept test results from any ONC-Authorized Testing Laboratory in good standing under the Certification Program and compliant with certain accreditation requirements.

c. Health IT for the Care Continuum

Certification Criteria for Pediatric Care Settings

- ONC identified the existing 2015 CEHRT criteria and the new or revised criteria that support the voluntary certification of health IT modules for pediatric care and pediatric settings.

d. Conditions and Maintenance of Certification Requirements

Information Blocking

- ONC adopted the Information Blocking Condition of Certification requirement prohibiting any health IT developer from taking any action that constitutes information blocking. Developers could face removal from the certification program if they are found to be information blocking.

Assurances

- ONC finalized several Conditions of Certification and Maintenance requirements to provide assurances to the Secretary that, unless for legitimate purposes as specified by the Secretary, the developer will not take any action that constitutes information blocking or any other action that may inhibit the appropriate exchange, access, and use of EHI.

Communications

- The Cures Act required ONC to develop Conditions and Maintenance of Certification requirements that health IT developers do not prohibit or restrict communications about certain aspects of the performance of health IT and the developers' related business practices. These include: usability, interoperability, security, user experience, and business practices related to exchange of EHI, and the manner in which the user of the health IT has used such technology.
- ONC finalized provisions that allow health IT developers certified under the Program to place limitations on certain types of communications, including screenshots and video:
    - Allows developers to limit the sharing of screenshots to only the relevant number needed to communicate about health IT.
    - Developers can impose restrictions on the communication of screenshots that contain PHI.
    - Communicators of screenshots must not alter the screenshots.
    - Developers can limit sharing of screenshots. ONC has retained the concept of "fair use" as it applies to all health IT developer intellectual property under "permitted prohibitions and restrictions" – it must pass a two-part test:

    - First, the communication that is being prohibited or restricted must not fall within a class of communications that is considered to always be legitimate or reasonable – such as communications required by law, made to a government agency, or made to a defined category of safety organizations.
    - Second, to be permitted, a developer's prohibition or restriction on communications must also fall within a category of communications for which it is both legitimate and reasonable for a developer to limit the sharing of information about its health IT.
- A health IT developer must not impose or enforce any contractual requirement that contravenes the requirements of this Condition of Certification.
- If a health IT developer has contracts/agreements that contravene the requirements of this Condition of Certification, the developer must notify all affected customers, other persons, or entities that the prohibition or restriction within the contract/agreement will not be enforced by the health IT developer.

APIs

- ONC adopted new standards, implementation specifications, certification criterion, and modified the Base EHR definition to meet the statutory API requirements.
- The new certification criterion will replace the "application access – data category request" criterion, requires standardized API access for single patient and population services, and is limited to "read-only" services. Additional requirements for health IT developers and certified API technology include:
    - **Base Standard:** HL7 FHIR Standard Release 4.0.1;
    - **Data Access and Search:** For both single and population-level services, the API is required to respond to requests for data specified to the USCDI v1 according to the HL7 FHIR US Core Implementation Guide (IG). The API must support "group-level export" for multiple patients' data according to the Bulk Data Access IG. The API will need to support all required search criteria specified to FHIR US Core IG for access requests with patient and user scope;
    - **Software App Registration:** Third-party apps will need to be registered with the API's "authorization server" prior to interacting with the API;
    - **Publicly Accessible Technical Documentation:** the API must make all technical documentation necessary for developers to design and register apps that interact with the API available via a publicly accessible hyperlink;
    - **Security:** The API must establish a secure and trusted connection with the app and must perform additional authentication and authorization using stated implementation specifications before clinicians can use the app for clinical purposes or before an app is authorized for patients to receive their information;
    - **Patient Authorization Revocation:** When directed by a patient, the API's authorization server must be able to revoke an authorized app's access to that patient's information;
    - **Token Introspection:** API authorization server must provide capability to receive and validate tokens it has issued;
    - **Permitted Fees:** Health IT developers can charge fees to clinicians that deploy the API (including usage costs), and can also charge app developers for certain services; and
    - **Openness and pro-competitiveness:** Health IT developers must follow certain practices that enable an open and competitive app marketplace.

Real World Testing

- Established new real world testing Condition and Maintenance of Certification requirements for health IT focused on interoperability and data exchange.

- Health IT developers must submit publicly available annual real-world testing plans, as well as annual real-world testing results for these criteria.
- Under Standards Version Advancement Process (SVAP), developers will have the option to update their health IT that is certified to these criteria or use more advance version(s) of the adopted standard(s) or implementation specification(s) included in the criteria, provided such versions are approved by the National Coordinator for use in health IT certified under the Program.
- Health IT developers presenting health IT for initial certification to one of these criteria would have the option to certify National Coordinator-approved newer version(s) of one or more of the Secretary-adopted standards or implementation specifications applicable to the criterion.
- All developers voluntarily opting to avail themselves of the SVAP flexibility must ensure that their annual real-world testing plans and real-world testing results submissions address all the versions of all the standards and implementation specifications to which each Health IT Module is certified.
- Health IT developers that wish to avail themselves of the SVAP flexibility must notify both their ONC-ACB and their affected customers of their plans to update their certified health IT, and the update's anticipated impact on their existing certified health IT.
- Added new PoPC for ONC-ACBs that requires ONC-ACBs to review and confirm that each health IT developer with one or more Health IT Module(s) certified to any one or more of the exchange criteria submits real-world testing plans and real-world results on a timeframe that allows for the ONC-ACB to confirm completeness of all plans and results by applicable annual due dates.
- Added to PoPC requirement that ONC-ACBs aggregate and report to ONC no less than quarterly all updates successfully made to support National Coordinator-approved newer versions of Secretary-adopted standards in certified health IT pursuant to the developers having voluntarily opted to avail themselves of the SVAP flexibility.
- Require ONC-ACBs to ensure that developers seeking to take advantage of the SVAP flexibility provide advance notice to all affected customers and its ONC-ACB.

Attestations

- Developers will be required to attest twice a year to all other Conditions of Certification, except for the "EHR Reporting Criteria submission" that is not yet developed.
- Attestations are submitted to the ONC-ACBs, then made publicly available through the CHPL.

EHR Reporting Program Criteria

- ONC has yet to develop a reporting criterion as required by the Cures Act. Once the program is established, ONC will undertake rulemaking and implement the associated Condition and Maintenance of Certification requirements for health IT developers.

Corrective Action Process

- ONC finalized proposed corrective action process to review potential or known instances where a Condition of Certification or Maintenance requirement has not been met or is not being met by a health IT developer. The ONC Direct Review of Certified Health IT will be used in the enforcement.

e. Information Blocking

Information Blocking Definition

- To meet statutory definition of information blocking, a practice must be likely to interfere with, prevent, or materially discourage the access, exchange, or use of EHI.
    - **Access:** the ability or means necessary to make EHI available for exchange, use, or both.

- **Exchange:** the ability for electronic health information to be transmitted between and among different technologies, systems, platforms, or networks.
- **Use:** the ability for EHI, once accessed or exchanged, to be understood and acted upon.

Actors subject to information blocking enforcement:

- Health care clinicians;
- Health IT developers of certified health IT: An individual or entity that develops or offers certified health IT (excludes health care providers who self-develop health IT for their own use); and
- Health Information Networks and Health Information Exchanges: Combined definitions of HIN and HIE to create one functional definition – an individual or entity that determines, controls, or has the discretion to administer any requirement, policy, or agreement that permits, enables, or requires the use of any technology or services for access, exchange, or use of EHI: (1) among more than two unaffiliated individuals or entities (other than the individual or entity to which this definition might apply) that are enabled to exchange with each other; and (2) that is for a treatment, payment, or health care operations purpose. This is not limited to individuals or entities that are covered entities or business associates under HIPAA.

Information Blocking Exceptions

- The 21st Century Cures Act requires ONC to define actions that do not constitute information blocking.
- Exceptions are limited to certain activities that ONC believes are important to the successful functioning of the US health care system, including promoting public confidence in health IT infrastructure by supporting the privacy and security of EHI, and protecting patient safety and promoting competition and innovation in health IT and its use to provide health care services to consumers.
- Each exception is intended to address a significant risk that regulated individuals and entities will not engage in these reasonable and necessary activities because of potential uncertainty regarding whether they would be considered information blocking.
- Each exemption 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.
- ONC finalized eight exceptions that describe when a practice shall not be treated as information blocking if the actor satisfies an exception to the provision by meeting all applicable requirements and conditions of the exception at all relevant times. The eight exceptions fall into two categories:
  - 1) exceptions that involve not fulfilling requests to access, exchange, or use EHI; and
  - 2) exceptions that involve procedures for fulfilling requests to access, exchange, or use EHI.
- Failure to meet the conditions of an exception does not automatically mean a practice constitutes information blocking. Instead, it is evaluated on a case-by-case basis to assess the specific facts and circumstances to determine whether information blocking has occurred.

Table 1: Information Blocking Exceptions and Descriptions

Not fulfilling requests to access, exchange, or use EHI	
Exception	**Description**
Preventing Harm	The actor engaging in the practice must hold a reasonable belief that the practice will substantially reduce a risk of harm to a patient or another natural person that would otherwise arise from the access, exchange, or use of electronic health information affected by the practice, and must meet the specified conditions.
Privacy	An actor's practice of not fulfilling a request to access, exchange, or use electronic health information in order to protect an individual's privacy will not be considered information blocking when the practice meets all of the requirements of at least one of the sub-exceptions. (See "Allowable Third-Party App Vetting" section below.)
Security	An actor's practice that is likely to interfere with the access, exchange, or use of electronic health information in order to protect the security of electronic health information will not be considered information blocking when the practice meets the specified conditions. (See "Allowable Third-Party App Vetting" section below.)
Infeasibility	An actor's practice that is likely to interfere with the access, exchange, or use of electronic health information in order to protect the security of electronic health information will not be considered information blocking when the practice meets the specified conditions.
Health IT Performance	An actor's practice that is implemented to maintain or improve health IT performance and that is likely to interfere with the access, exchange, or use of electronic health information will not be considered information blocking when the practice meets the specified conditions.
Procedures for fulfilling requests to access, exchange, or use EHI	
Exception	**Description**
Content and Manner (NEW within FINAL RULE)	An actor's practice of limiting the content of its response to or the manner in which it fulfills a request to access, exchange, or use electronic health information will not be considered information blocking when the practice meets the specified conditions.
Fees	An actor's practice of charging fees, including fees that result in a reasonable profit margin, for accessing, exchanging, or using electronic health information will not be considered information blocking when the practice meets the specified conditions.
Licensing	An actor's practice to license interoperability elements for electronic health information to be accessed, exchanged, or used will not be considered information blocking when the practice meets the specified conditions.

Definition of electronic health information (EHI)

- In the final rule, ONC narrowed the definition of EHI to align with the definition of electronic protected health information (ePHI) under HIPAA.
- ONC also added an exception that allows an actor to provide, at a minimum, a limited set of EHI comprised of the data elements included in the USCDI for access, exchange, and use during the first 18 months after the compliance date of the information blocking provisions (24 months after publication of the final rule).
- There was discussion of whether to include price information in the definition of EHI. By limiting to the definition of ePHI, it would not include price information unless it is included in a designated record set.
    - The definition of EHI also does not specifically include or exclude algorithms or processes that create EHI, clinical interpretation, or relevancy of the results of the algorithms or processes.
    - Also, in accordance with HIPAA, de-identified information is not considered EHI.

Privacy and Security Exception – Allowable Third-Party App Vetting by Clinicians

- For certified API technology, there should be few, if any, security concerns about the risks posed by patient-facing apps to the disclosing actor's health IT systems (because the apps would only be permitted to receive EHI at the patient's direction).
- **Patient-mediated exchange:** For third-party apps chosen by patients to facilitate their access to their EHI held by clinicians, there would generally not be a need for "vetting" by clinicians on security grounds. Such vetting actions otherwise would be an interference (**or information blocking**), which distinguishes vetting from verifying an app developer's authenticity under the API Condition of Certification.
- **Clinician-mediated exchange:** Actors, such as clinicians, do have the ability to conduct whatever "vetting" they deem necessary of entities (app developers) that would be their business associates under HIPAA before granting access and use of EHI to the entities. The HIPAA Security Rule requires this.
- Clinicians are able to provide additional information to individuals about apps to assist individuals as they choose apps to receive their EHI. Such an approach is consistent regarding informing individuals about the advantages/disadvantages of exchanging EHI and any associated risk.
    - Practices that purport to educate patients about the privacy and security of practices of apps and parties to whom a patient chooses to receive their EHI may be reviewed by OIG or ONC, as applicable, if there was a claim of information blocking.
    - The information provided by actors must focus on any current privacy and/or security risks posed by the technology or the third-party developer of the technology.
    - The information must be factually accurate, unbiased, objective, and not unfair or deceptive.
    - The information must be provided in a non-discriminatory manner.
    - An actor may not prevent an individual from deciding to provide its EHI to a technology developer or app, despite any risks noted regarding the app itself or third-party developer.

f. Enforcement

Responsible Parties

- ONC is solely responsible for enforcing compliance with the Conditions and Maintenance of Certification requirements.
- The Cures Act authorizes OIG to investigate claims that a health IT developer of certified health IT has engaged in information blocking.
- ONC and OIG are actively coordinating on establishing referral policies and procedures to ensure the timely and appropriate flow of information related to information blocking complaints.
- Enforcement of information blocking civil monetary penalties (CMPs) will not begin until established by future notice and comment rulemaking by OIG.
- The Cures Act also requires ONC to implement a standardized process for the public to submit reports on claims of health information blocking. ONC is working to build off these existing processes.

IV. Timelines

- **May 1, 2020** – Final regulations published in Federal Register
- **June 30 2020 – GENERAL EFFECTIVE DATE of ONC RULE:** 60 days after official publication in FR
    - Vendor Requirements:
        - Condition of Certification – Assurances (Other)
        - Condition of Certification – Communications
            - Health IT vendors prohibited from restricting certain communications (gag clauses, screenshots, videos) (**3 month enforcement discretion**)
- **November 1, 2020** – 6 months after publication
    - Clinician Requirements:
        - Information Blocking Compliance (**no enforcement discretion**)
            - EHI definition limited to USCDI for 18 months
    - Vendor Requirements:
        - Condition of Certification – Information Blocking deadline for vendors (**3 month enforcement discretion**)
        - Condition of Certification – Assurances
            - Will not take any action that constitutes information blocking or actions that inhibit access, exchange, and use of electronic health information (EHI). (**3 months enforcement discretion**)
        - Condition of Certification – API
            - Compliance by Certified API developers with health IT certified to current API criteria (**3 month enforcement discretion**)
- **December 15, 2020**
    - Deadline for Vendor First Real-World Testing Plans Due (**extension through March 15, 2021**)
- **April 1-30, 2021**
    - Vendor Requirements
        - Conditions of Certification – Initial Attestations (**extension through July 30, 2021**)
- **May 1, 2022 –** 24 months after publication in FR
    - Clinician Requirements
        - Information Blocking Compliance
            - Full EHI definition in effect
    - Vendor Requirements
        - Condition of Certification – API
            - New HL7 FHIR API Capability and Other Cures Update Criteria Must be rolled out (**3 month enforcement discretion**)
        - Condition of Certification – Real-World Testing
            - Updates to USCDI (**3 month enforcement discretion**)
- **May 1, 2023 –** 36 months after publication in FR
    - Vendor Requirements:
        - Condition of Certification: Assurances
            - EHI Export capability must be in place (3 month enforcement discretion)