Interoperability MATTERS
an initiative of The Sequoia Project

Good Practices for Information Sharing and Information Blocking Compliance

September 19, 2022

the sequoia project

Contents

Note: The materials developed by the IBWG are intended to be educational and informational resources. These materials will be most helpful to those who have a strong understanding of the regulatory requirements but seek to understand real-world implications and approaches to implementation. They are not, and are not intended to, constitute legal advice or a treatise on the Information Blocking Rule. Regulated Actors are encouraged to seek appropriate counsel to advise on the Actor's legal compliance. No Actor should act or refrain from acting on the basis of the IBWG materials without first seeking legal advice from counsel. All liability with respect to actions taken or not taken based on the IBWG materials are hereby expressly disclaimed. The IBWG materials are provided "as is;" no representations are made that the content is error-free.

© 2022 The Sequoia Project. All rights reserved

Interoperability MATTERS
an initiative of The Sequoia Project

Good Practices: An Overview

© 2022 The Sequoia Project. All rights reserved

Development of Good Practices

This document provides Good Practices for Actors that must comply with the Information Blocking rules issued by the Office of the National Coordinator for Health IT (ONC). It was created by the Information Blocking Compliance Workgroup (IBWG) of The Sequoia Project's Interoperability Matters Cooperative, with the assistance of additional subject matter experts. This work reflects the experience of the individuals who volunteered their time and expertise to share operational experiences and approaches. We especially thank the following individuals who worked on the Good Practices Task Group: (*Co-chairs)

Health Information Networks & Service Providers: Rene Cabral-Daniel, Kevin Conway, Daniel Kim, Dan Paoletti, Pat Russell, Melissa Soliz, Alan Swenson, Sylvia Trujillo

Healthcare Providers / Physicians: Jeffrey Alex, Roberta Baranda, Casey Bryson, Matthew Eisenberg, Ammon Fillmore*, Eric Liederman, Bridget Leon, Virginia Lorenzi, Sid Thornton, Suzanne Srebnik

Developers: Matt Becker*, Rita Bowen*, Alex Desilets, Leigh Burchell, Stephanie Jamison, Josh Mast, Ladd Wiley

Associations and Organizations - Health IT Community: Jeff Coughlin, Matt Reid

Consumers/Data Requesters: Jennifer Blumenthal, Deven McGraw

We also encourage readers to review complementary IBWG materials on the 10/6/2022 shift, for Information Blocking compliance, to the full definition of Electronic Health Information (EHI) based on the Designated Record Set. In particular, we encourage review of the report on operational implications of this broader definition.

© 2022 The Sequoia Project. All rights reserved

Why Good Practices?

- The Good Practices in this document are intended to: enhance the speed and effectiveness of Actor organizations' planning and implementation for compliance with the ONC information blocking regulations, enable wider and more effective healthcare information sharing, and expand opportunities to meet customer and patient needs.

- Good Practices can reduce compliance costs, draw on knowledge and experiences across the industry and Actor types, and increase the consistency and usefulness of health care information sharing.

- Finally, Good Practices can be of particular use to smaller organizations and those in earlier stages of information blocking compliance; these Good Practices were developed with such users in mind.

© 2022 The Sequoia Project. All rights reserved

Working with Good Practices

- The Good Practices Task Group identified a broad and deep set of Good Practices for priority compliance issues.
- These Good Practices are not legal advice nor authoritative or comprehensive regulatory summaries or analyses. They reflect published materials and information as of the publication date. We encourage users to review the regulatory summary in the Appendix and other materials identified on page 120. (ONC and the HHS OIG have forthcoming proposed and final rules relating to information blocking and may also issue additional regulatory guidance).
- These Good Practices are a ***super-set*** of practices that may be applicable and useful for specific organizations; they are not presented as a compliance floor nor with the expectation that all will be adopted by any organization.
- Most are directly or indirectly applicable to all Actor types, and, in some instances, to organizations that interact with Actors. Some Good Practices are, however, most applicable to specific Actor types and are so identified.
- Finally, we recognize that Actor organizations vary widely in size, structure, health care focus, and experience with information blocking compliance–as a result, these Good Practices are, in general, designed to be scaled (up or down) and should be adapted based on Actor characteristics and needs.

© 2022 The Sequoia Project. All rights reserved

Information Sharing Good Practices: An Overview

- The Good Practices Task Group conducted a prioritizing analysis of issues for which Good Practices would be valuable to the industry.
- In doing so, it focused on two dimensions: (1) *Importance to Stakeholders* and (2) *Ability to Have an Impact.* The Task Group centered its work on three issues scoring high on both dimensions, while bringing into its analysis other relevant priority issues.
- This report addresses the three highest priority issues:
  - Compliance planning and implementation, including responding to complaints of information blocking
  - Identifying, managing, responding to Electronic Health Information (EHI) requests, including Individual Access
  - Using Exceptions
- Within these topics, the Good Practices also address compliance with state and local law, contracts and HIPAA Business Associate Agreements (BAA), and usability.

© 2022 The Sequoia Project. All rights reserved

Key Themes

- Organizations that are Actors or interact with Actors face many risks and opportunities from the ONC information blocking regulations.
- They will need formal, organization-wide plans for compliant and effective operational and business responses to these regulations.
- In addition to compliance responsibilities, Actors should consider how these regulations might affect their own data requests to other Actors and related business relationships.
- Successful responses require engagement and support from the highest levels of an Actor organization and across its teams.
- These responses should emphasize consistent and high-quality documentation.
- Actors should prioritize documented intent to share when possible, avoiding discriminatory or anti-competitive behaviors, and a culture of authorized information sharing.
- Use of Good Practices can reduce compliance costs, draw on knowledge and experiences across the industry and Actor types, and increase health care information sharing.
- Because Actor organizations vary widely on key dimensions relevant to compliance, they should choose from and adapt these Good Practices based on their particular characteristics and needs.

© 2022 The Sequoia Project. All rights reserved

Interoperability MATTERS
an initiative of The Sequoia Project

Good Practices: Compliance Planning and Implementation

© 2022 The Sequoia Project. All rights reserved

Compliance Planning and Implementation

I. Checklists, sample policies, workflows
II. Ensuring clear issue ownership within the organization (e.g., who owns which compliance steps)
III. Organizational issues (e.g., roles of senior management, HIM, legal)
IV. Responding to complaints of information blocking

© 2022 The Sequoia Project. All rights reserved

Checklists, Sample Policies, Workflows

- Good Practice: Create a centralized “funnel” process to capture potential EHI requests for further evaluation by the appropriate workflows and SMEs, without front-line staff needing to determine whether a valid request for EHI has been made. [All Actor-types]
  - Requests may come from many sources in addition to patient portals, including multiple *internal* staff and units (e.g., payer relations, public health, API* requests to IT), reinforcing the need for broad staff training and a centralized intake and request evaluation function. These request handling processes can help demonstrate **intent** for information sharing and compliance.
  - If a data requester, team member or other person raises concerns about “information blocking,” make sure that all relevant staff understand what that term means and how to get help from the right team members.

*Application Programming Interfaces

© 2022 The Sequoia Project. All rights reserved.

Checklists, Sample Policies, Workflows

- Good Practice: Create processes that do not depend on a specific staff interpretation of an EHI "request" or require an identified "request" to trigger workflows, which should be initiated by acts or omissions that **affect access, exchange, or use of EHI.** [All Actor-types]
  - ONC has not fully defined what is or is not a request, notably for portal access (e.g., is a portal log-in a request for some EHI, specific EHI, or all EHI?).
  - ONC has also emphasized, especially in recent FAQ 3.1.2022FEB, that failure to comply with an applicable state or federal law could be information blocking. It has also emphasized the role of security practices, fees, licensing, Business Associate Agreements (BAAs) in implicating information blocking.

© 2022 The Sequoia Project. All rights reserved.

Checklists, Sample Policies, Workflows

- Good Practice: Create training and compliance programs for staff who are not part of the regular Health Information Management (HIM)/Release of Information (ROI)/EHI access process but who might receive EHI requests or have responsibilities for activities that could implicate information blocking (e.g., ancillary staff, pricing specialists, contract and procurement teams, legal teams, interface engineers, security teams, etc.). This training should address the role of these teams with respect to applicable exceptions, including Fees, Licensing, Security, Content and Manner and Infeasibility. [All Actor-types]
  - Include these teams in information blocking compliance workflows.
  - Update workflows and checklists used by these teams to ensure that information blocking compliance is addressed.

© 2022 The Sequoia Project. All rights reserved.

Checklists, Sample Policies, Workflows

- Good Practice: Create workflows for routine and non-routine EHI requests. *Routine requests* should generally be handled by regular Health Information Management (HIM), Release of Information (ROI) or EHI access processes. *Non-routine requests*, including requests for large amounts of EHI (data elements or patients) that cannot be handled through standard processes, should have specific workflows appropriate to the organization to ensure that the Actor addresses applicable circumstances, including the requirements of exceptions, such as timeliness requirements (e.g., Infeasibility and Licensing). [All Actor-types]

- Good Practice: Customize ROI templates for the needs of specific Actor organizations and Actor categories, especially considering the full range of relevant state and federal laws and regulations.
  - Providers (and other Actors) may develop workflows and forms to separately support "HIPAA patient access requests" as well as "HIPAA authorizations".
  - For example, ROI processes that support individual patient access requests (vs. a full HIPAA authorization) might work well for providers with an EHR, but for HIEs/ HINs that have aggregated data repositories, with data from a wide variety of sources (not just an EHR), a HIPAA authorization is likely needed.
  - Disclaimers will be important because ROI processes won't necessarily be tailored to the requirements of more stringent privacy laws (e.g., 42 CFR Part 2 and state "sensitive data" laws).

© 2022 The Sequoia Project. All rights reserved.

Checklists, Sample Policies, Workflows

- Good Practice: Create an organizational tool kit to *communicate* with patients, team members, other stakeholders and data requesters on the Actor's approach to information sharing and to information blocking compliance
  - Especially for Provider Actors, it will be important to communicate to team members that it is welcome and desirable for patients to access and engage with their health data and that **information sharing** is the organization's goal.
- Good Practice – For Provider Actors, suggest to patients that they should access, review, and use their data and provide patients with information and assistance to enable such data access and use.
- Good Practice: Create policies and procedures for redisclosure of externally developed data that has been received, including use of provenance information.
  - These policies are especially important when portions of received CCDs/summaries have been **integrated into the patient record**.
  - It will also be important to create policies and procedures to track and document data provenance and to create inventories of organizations contributing external summary documents.

© 2022 The Sequoia Project. All rights reserved.

Checklists, Sample Policies, Workflows

- Good Practice: Create a “button” on the Actor organization’s website and/or portal to handle EHI requests that are not satisfied by portal access or ongoing connectivity.
  - The button on the portal or website would take the user to an intake form, which could initiate a different response path depending on the type of requester (e.g., patient, attorney, provider, app developer, etc.).
    - This intake form should request, using simplified language, the information needed to fully define and evaluate the EHI request and ensure that it is complete and can be acted on per the Actor’s requirements.
    - The completed intake form should trigger an Actor organization’s workflow, consistent with the Actors processes, considering, for example the type of EHI requested and the party requesting the data.
  - Organizations may choose to have the same or different processes and forms depending on requester-type but should ensure a solid privacy-based rationale if different categories of requesters are treated differently.
  - Organizations should consider whether to identify specific data elements available on the portal or request form or to be general as to the types of available information (on the portal or otherwise).
  - Being proactive in making patients’ information easily available to them has important equity and disparity reduction implications.
  - Patient matching issues must be carefully addressed, especially for HIEs/HINs.

© 2022 The Sequoia Project. All rights reserved.

Ensuring Clear Issue Ownership within Organization

- Good Practice: Establish workflows and lines of responsibility for specific information blocking compliance issues. These will vary by the Actor-type, size of the organization, and other factors.
  - For example, exceptions might go the Compliance Officer and/or an Exceptions Review Committee, patient requests to the HIM Director, payer requests to Payer Relations, and provider requests to Provider Relations.
  - Actor organizations, including Developers in particular, should consider models where, in addition to more centralized functions, such as for security and privacy, subject matter experts (SMEs) and operating units have defined “ownership” for appropriate aspects of information blocking compliance.

- Good Practice: Create a clear process and forms to manage and document use of exceptions, including, resources permitting, a cross-walk between specific exceptions and other applicable policies (e.g., if a requested authorization is not HIPAA compliant, point to the Privacy exception). [All Actor-types]

- Good Practice – Provider Actors should coordinate with their Release of Information (ROI) fulfillment and request tracking functions. Those without a robust portal or APIs connected to apps like Apple® Health are likely at higher risk of sub-optimal request management.

© 2022 The Sequoia Project. All rights reserved.

Ensuring Clear Issue Ownership within Organization

- Good Practice: Establish a clear understanding and policy on the role of the patient or provider portal (or other Actor controlled portals) in information blocking requests.
  - Adopt a vision and culture of "let's make everything available that we can via the portal" and work internally and with developers and vendors to expand the information that can be provided through the portal.
  - Policy, guidance and portal request workflows should be aligned with the organization policies on HIPAA right of access requests (including the ability of the covered entity to dictate how requests must come in) and with organizational information blocking-related policies.
  - Provide clear information **in the portal** (e.g., in **terms of use**) on what EHI can generally be expected to be found in the portal (e.g., problems, medications, clinical notes, and other CCDS/USCDI v1 data elements) and what EHI (USCDI v1 data set or beyond) is always or often not available in the portal (e.g., because it is not required of certified portals or exists in systems that are not linked to the portal, such as those other than the main EHR).
  - Recognize and communicate to patients that the portal is not the only way that patients can access their EHI, even if the information is available on the portal.

Continued on next page

© 2022 The Sequoia Project. All rights reserved.

Ensuring Clear Issue Ownership within Organization

Continued from prior page

- Consider a process that transparently informs the patient **when they log into the portal** that certain specific types of information can be expected to be found on the portal and that, to access other records, they should complete an indicated form.
- **Be clear, up front**, with the patient/personal representative about what cannot be provided in the portal. To handle EHI that the patient/personal representative still wants or needs, provide clear information in documentation and portal **terms of use** on how to request such EHI or to contact the organization for how/if they can get the information electronically if needed.
- Similarly, create a process, potentially using the portal, to notify a patient if information that would otherwise be expected to be in the portal is not available and **how it can be accessed or what exception applies**. This process *could* be triggered by a portal log-in.
- More specifically, for information not available through the portal, or not found when expected, provide portal users with clear instructions and contact information (e.g., hyperlinks, email addresses, phone numbers, forms) on how to request the desired EHI from HIM or another appropriate source and what information is needed to process requests. This approach could include a specific link/form for images (e.g., x-rays).

© 2022 The Sequoia Project. All rights reserved.

Organizational Issues

- Good Practice: Involve organizational governance and leadership in information blocking compliance. [All Actor-types]
- Good Practice: Recognize that data access and information blocking compliance is a “whole of organization” responsibility and not only or even primarily the responsibility of the HIM/legal/compliance functions. [All Actor-types]
- Good Practice: In particular, involve patient/user experience leadership in information blocking compliance. [All Actor-types]
- Good Practice: Assign lead unit(s) to monitor use of specific exceptions to ensure exceptions are used only when indicated, meet timeliness criteria, and are documented (e.g., HIM monitors Preventing Harm and Privacy; marketing/pricing/legal address Fees and Licensing). This monitoring process could also look for trends and root causes. [All Actor-types]

© 2022 The Sequoia Project. All rights reserved.

Organizational Issues

- Good Practice: Create an organizational culture, including education, training and communications, that focuses on maximizing information sharing rather than “not information blocking”. [All Actor-types]
- Good Practice: Educate staff on how the patient or other portal fits into information sharing strategies and that not having information on the portal does not mean that information blocking is occurring.
- Good Practice: Educate the workforce on how to deal effectively with patients who seek their information, encouraging such access and use.
- Good Practice: Educate staff on the exceptions and their role in appropriate and compliant use of exceptions. [All Actor-types]
- Good Practice: Educate staff on when they cannot share requested data, based on legal, contractual, or regulatory grounds and on the proper escalation paths when such issues arise ((e.g., to legal or an Information Blocking committee). Use outside legal counsel as needed to augment internal resources and expertise. [All Actor-types]

© 2022 The Sequoia Project. All rights reserved.

Organizational Issues

- Good Practice: The HIM function should identify requests that it receives that have potential information blocking compliance issues (e.g., if a patient tried and failed to find the information on the portal) and share this risk and needed steps with appropriate other units (e.g., privacy, compliance, legal, etc.).

- Good Practice: Ensure that non-Actor contractors, HIPAA *Business Associates*, partners and others whose actions can affect an Actor's obligations and compliance risks understand and are trained on information blocking requirements (e.g., HIT developers and contractors, both "certified" and "non-certified").

© 2022 The Sequoia Project. All rights reserved.

Organizational Issues

- Good Practice: Work with legal counsel to address needed organizational, legal, and management issues when an organization has units or lines of business that include **multiple Actor categories**, including clear lines of organization and responsibility (e.g., Provider and Developer). [All Actor-types]

- Good Practice: Actors (e.g., Providers) that act as **resellers or distributors of certified HIT** may fall into the Developer Actor category and must plan accordingly.

© 2022 The Sequoia Project. All rights reserved.

Responding to Complaints of Information Blocking

- Good Practice: Actors should engage proactively to both head off and respond to complaints, including by **pledges** to support information sharing (widely communicated within and outside of the organization) and **scripts** that can be used by Actor staff to respond to both EHI requests and complaints, consistent with organizational policy. [All Actor-types]
  - Scripts can be used by both clinical staff and non-clinical staff (e.g., to inform patients that they may see test results in the portal before a discussion with their clinician; that a new mother's EHI may also be in her newborn's record, accessible to the father).
  - Scripts can also highlight an organization's intent to share "responsibly" while also indicating when information cannot be shared due to legal or other obligations to keep the patient safe; known infeasibility issues; the need to meet privacy/security requirements (e.g., no legacy system data in portal, no access without agreeing to a Participation Agreement, etc.); and providing disclaimers that the releasing organization is not the source of the data (e.g., because it is imported from a health information exchange (HIE)).
  - Add information to these scripts on portal access, what data may not be available in the portal and why, and how to access non-portal information
  - Create a diagram or flow-chart for internal planning and training on pledges and scripts regarding what potentially requested EHI is available from which source (e.g., portal, ROI, archived data, etc.).

© 2022 The Sequoia Project. All rights reserved.

Responding to Complaints of Information Blocking

- Good Practice: Be honest with data requesters when release of EHI may be more complicated than usual or expected by the requester.
- Good Practice: It is essential to recognize and act on the importance of **intent and knowledge** in determining whether information blocking has occurred for compliance purposes, especially for Providers who have a different standard for these factors than other Actors.
- Good Practice: It will be helpful to engage in a thoughtful review of the applicable information blocking regulatory provisions with data requesters who have **non-routine or complex requests** whose handling may raise concerns with potential information blocking.
  - For example, emphasize that these rules do not impose strict liability or take a binary "all or nothing“ approach; in fact, the regulatory language reflects complexity and nuance.

© 2022 The Sequoia Project. All rights reserved.

Responding to Complaints of Information Blocking

- Good Practice: Be prepared to address complaints, especially from patients (e.g., to Providers), or Providers (e.g., to Developers, HIEs/HINs) that they are receiving too much or non-usable information as a result of an Actor's information blocking compliance efforts.

- Good Practice: Use **table-top exercises** to test and refine complaint response processes.

- Good Practice: Review data on the nature, volume, and expected (by requesters) response times of prior Protected Health Information (PHI) requests to guide the nature and timing of Actor organizational investments to make additional data available in the portal; use the same type of analysis regarding what data to archive and when. (Table-top exercises also can be used to review these data.) Link this review to potential use of the Infeasibility exception.

© 2022 The Sequoia Project. All rights reserved.

Responding to Complaints of Information Blocking

- Good Practice: Treat information blocking complaints as "incidents“ per current organization practices for incident handling (especially re: PHI).
  - Create an accurate record that can be used to demonstrate that the Actor is trying to “do the right thing”
- Good Practice: In order to both reduce the number of complaints and to respond to complaints effectively, shift organizational culture and processes from a focus on compliance and data protection to one where the default is to embrace the spirit of the information blocking rule and to share whenever possible, per patient direction or compliance state and federal law.

© 2022 The Sequoia Project. All rights reserved.

Responding to Complaints of Information Blocking

- Good Practice: Developers, Providers and HIEs/HINs should utilize Developers' user groups to identify and discuss issues before they rise to the level of complaints to any of these parties.

- Good Practice: Like with other compliance programs, conduct regular **risk assessments** and use external audits and/or event simulations to review compliance adequacy (e.g., as applicable, HIPAA and privacy vendors could incorporate information blocking assessment into periodic privacy and security program assessments.). This practice should also include a review of correspondence being sent by a provider's HIM/ROI vendors.

© 2022 The Sequoia Project. All rights reserved.

Interoperability MATTERS
an initiative of The Sequoia Project

Identifying, Managing, Responding to EHI Requests, including Individual Access

© 2022 The Sequoia Project. All rights reserved.

Identifying, Managing, Responding to EHI requests

I. General EHI request response issues
II. Episodic vs. ongoing requests
III. Is it information blocking?
IV. EHI in multiple systems controlled by an Actor
V. Prioritizing types of requests
VI. Documentation
VII. Archived systems
VIII. Individual Access requests

© 2022 The Sequoia Project. All rights reserved.

General Request Response Issues

- Good Practice: Organize staff and processes to **timely answer** patient and other requester questions and encourage and help patients access their data in and navigate the Actor's patient portal (where applicable).
- Good Practice: Treat assistance to patients in accessing their health data as a key **patient engagement** function. [Providers]
- Good Practice – Actors and their health IT developers should work to create a **culture of information sharing** and to develop patient-facing and data requester-facing tools, including enhanced patient portal navigation (e.g., links to the Release of Information (ROI) function and information to data requesters on how they may access EHI when authorized to do so).

© 2022 The Sequoia Project. All rights reserved.

Episodic vs. Ongoing EHI Requests

- Good Practice: Ensure that processes and standard operating procedures (SOPs) can handle the full range of EHI requests (e.g., one-time requests to the HIM/ROI function, one-time requests to the patient portal, ongoing data feeds to the patient portal, one-time API requests, and ongoing API requests). [All Actors]
  - Note: EHI requests can be broadly divided into three categories:
    1. Use of health IT systems, including EHRs, are configured to provide EHI access via HIE connectivity, a portal or API/apps with a valid, automated request (also includes connectivity with public health agencies and established point-to-point connections);
    2. Requests using established HIM/ROI processes and procedures; and
    3. Other (e.g., large, custom data queries; provisioning of a new app, etc.).
- Good Practice: Ensure that portal and API terms of use and provisioning reflect industry-standard security practices, including tokens and passwords that are only in effect for a limited period (e.g., 90-days). Create and document such policies to help meet the Security exception.

© 2022 The Sequoia Project. All rights reserved.

Is it Information Blocking?

- Good Practice: Document each specific request for EHI and any response(s) to the requester. If the Actor can only only meet part of the initial request, use the **Content and Manner** exception as applicable. Regardless of whether this exception is used, document, where applicable, when the requester accepts the Actor's response as acceptable. Ensure that all such documentation reflects the Actor's intent to be as responsive as legally permitted and feasible.

- Good Practice: Be mindful of ONC regulations and guidance on the **10-day timing** to use the Infeasibility exception and to meet the Licensing exception. Establish clear workflows to meet these timing requirements and to document timely responses. Also establish workflows for instances when 10-day timing cannot be met (e.g., because of an unsuccessful effort to use the Content and Manner exception) to demonstrate good intent through documentation of good faith efforts to respond timely (and to use the Content and Manner exception if that was the initial goal).

© 2022 The Sequoia Project. All rights reserved.

Is It Information Blocking?

- Note: ONC has stated publicly (at its April 13-14, 2022 Annual Meeting but not in writing) that the 10-day period for Infeasibility **starts after initial due diligence** (e.g., to clarify the request and to confirm that the requester is entitled to the EHI) has occurred; nonetheless, recognize that current regulatory language is clear that the Actor must provide a written response to the requestor within 10 business days of receipt of a request with the reason(s) why the request is infeasible.
- Note: ONC and OIG have emphasized the importance of **knowledge and intent** and that **facts and circumstances** of a potential information blocking practice will be considered in enforcement review, even if the Actor is not eligible to use the Infeasibility exception because they did not meet the 10-day time period for the response.
- Note: In the information blocking Final Rule, ONC states that "[a]s part of an information blocking investigation, ONC and OIG may consider documentation or other writings maintained by the Actor around the time of the request that provide evidence of the Actor's intent. Additional documentation would not permit the Actor to avail themselves of this exception, but ONC or OIG could examine the Actor's intent using this documentation when assessing the information blocking claim." https://www.federalregister.gov/d/2020-07419/p-2523

© 2022 The Sequoia Project. All rights reserved.

Requests for EHI in Multiple Systems Controlled by an Actor

- Good Practice: Recognize and organize for the fact that requested EHI may be in different HIT systems controlled by the Actor, different Actor departments, and different Actor sites.
- Good Practice: Recognize that patient generated health data (PGHD) can be part of EHI.
- Good Practice: Create a centralized request identification and response system that can help ensure that EHI requests with Actor-wide implications are identified and addressed even if the request came in through only one part of the Actor or one of its HIT systems.
- Good Practice: Recognize that the goal of information blocking regulations is to advance interoperability capabilities and therefore plan for prudent increases over time in the capacity to meet authorized EHI requests complicated by the fact that EHI is in multiple systems. Evaluate capabilities the Actor has in place currently and can or will have in place in the future and plan accordingly. Do not assume that **today's tools** are all that are needed.

© 2022 The Sequoia Project. All rights reserved.

Requests for EHI in Multiple Systems Controlled by an Actor

- Good Practice: In evaluating EHI requests and their scope, recognize that the **same EHI may be in different applications** (i.e., duplicated) and that it may be easier to access from one than others. Create documentation that can support such assessments for your organization.

- Good Practice: Recognize that the same information maintained in more than one location or system controlled by an Actor its business associate (i.e., duplicate information) is part of the DRS but in general, per the below notes, duplicate information need not be provided in response to a request, although doing so may be more convenient for the Actor.

- Good Practice: Recognize that provision of duplicate information to a patient, or for use cases like clinician use or population management exports, can reduce the usability and utility of that information and even obscure the fact that EHI is not available from some care sources.

© 2022 The Sequoia Project. All rights reserved.

Requests for EHI in Multiple Systems Controlled by an Actor

- Note: With respect to data that is maintained by an Actor in more than one HIT system or location, the HHS Office of Civil Rights has stated that "if the same PHI is maintained in more than one designated record set, a covered entity need only produce the information once in response to a request for access [by a patient]."

- Note: Similarly, ONC, in the Information Blocking Final Rule, has stated that ". . . .. if the same PHI that is the subject of an access request is maintained in both the designated record set of the covered entity and the designated record set of the business associate, the PHI need only be produced once in response to the request for access."" The citation used by ONC to support this position is from the regulations governing the individual right of access cited above.

© 2022 The Sequoia Project. All rights reserved.

Requests for EHI in Multiple Systems Controlled by an Actor

- Good Practice – Create Standard Operating Procedures (SOPs) to help requesters clarify their EHI access goals and what data they really want, and to help them to understand how it can be accessed. Such SOPs should be developed and in place **ahead of specific EHI requests** and then applied to the specific facts and circumstances of individual requests.

- Good Practice: If a request for EHI that is maintained in more than one location or system of an Actor also specifies a location/system that is less convenient or feasible to access than others, use the Content and Manner exception to work with requesters to provide EHI in an alternate mutually acceptable manner.

© 2022 The Sequoia Project. All rights reserved.

Requests for EHI in Multiple Systems Controlled by an Actor

- Good Practice: For eDiscovery and other applicable purposes, an Actor may wish to designate a “single source of truth” relevant to EHI access, exchange, and use; issues and policies in patient matching and data de-duplication should be part of this consideration.

- Good Practice: If the same EHI is maintained by multiple Actors, each Actor may have information blocking regulatory obligations to respond to requests, as well as obligations as a Business Associate (e.g., HIN or Developer) that may limit an Actor’s ability to respond.

© 2022 The Sequoia Project. All rights reserved.

Requests for EHI in Multiple Systems Controlled by an Actor

- Good Practice: In evaluating requests for EHI in multiple systems that it controls, an Actor should consider which of its lines of business are subject to information blocking compliance (i.e., meeting the definition of an "Actor") and also recognize that not all ePHI will meet the definition of the DRS or EHI (e.g., if it is "not used to make decisions about individuals. This may include certain quality assessment or improvement records, patient safety activity records, or business planning, development, and management records that are used for business decisions more generally rather than to make decisions about individuals.").

© 2022 The Sequoia Project. All rights reserved.

Prioritizing EHI Requests

- Good Practice: Be consistent in how similarly situated requesters are treated in both response timing and execution.
- Good Practice: Document any inability to respond positively to a request in a short time frame and why, especially if there is an applicable exception (e.g., system outages, the need to protect system performance, competing resources for app connection, etc.).
- Good Practice: Prioritize work on requests that are not well understood, given the tight response times for the Infeasibility and Licensing exceptions and the general requirement for timely response. Document the response request, the intent to respond positively if legally authorized and feasible, and why the time to respond was needed, even if it exceeds that required for an applicable exception. The initial review and response period should establish whether the requester has a legal right to the data (if they do not, then there is no **interference** and no exception is required).

© 2022 The Sequoia Project. All rights reserved.

Prioritizing EHI Requests

- Good Practice: Define, in advance, routine EHI requests that can be handled with established policy and SOPs to minimize costs and delays from special handling.
- Good Practice: Identify whether there are certain types of requests that cannot be met in whole or in part and create standard responses on why that is (consistent with regulations and related exceptions). Develop processes to respond to these requests with rapid turn-around.
- Good Practice: Establish a “request/response library” reflecting acceptable use cases for specific types of responses.

© 2022 The Sequoia Project. All rights reserved.

Prioritizing EHI Requests

- Good Practice: Consider the HHS OIG's finalized criteria (i.e., in the forthcoming HHS OIG Civil Monetary Penalty Final Rule) for which investigations to pursue and for establishing the size of Civil Monetary Penalties where prioritization of requests is needed given an Actor's limited time and resources to respond. These criteria are likely to include (as of August 2022) potential for harm, potential to cause patient harm, number of patients affected, negative impact on a provider's ability to care for patients, number of providers affected, duration of delayed response, financial loss to any federal healthcare program or other government or private entities.

© 2022 The Sequoia Project. All rights reserved.

Documentation of EHI Requests and Responses to Requests

- Good Practice: Document all responses, including those where the requested EHI is unavailable (e.g., the Actor does not maintain any EHI or the requested EHI).
- Good Practice: Create a central repository for all documentation and assign responsibility (e.g., Release of Information or HIM).
- Good Practice: If communications must be protected with legal privilege (e.g., due to risk of enforcement action or litigation), segregate relevant communications and limit to those with a “need to know” consistent with protection of the privilege.

© 2022 The Sequoia Project. All rights reserved.

Documentation of EHI Requests and Responses to Requests

- Good Practice: Ensure that policies for documentation are in writing, including for handling verbal requests (e.g., when a patient or other requester calls by phone for EHI).
- Establish internal documentation policies for routine requests that can be handled per policy that impose a lower burden on staff, with more detailed documentation requirements reserved for non-routine requests.
- Good Practice: Establish minimum documentation fields that can be **consistently applied** given Actor-type and organization size, the type of request, and an Actor's circumstances and capabilities
  - These fields could include some or all of the following: requester name, date/time, EHI requested, confirmation that the requested data is EHI, evaluation of state or federal law authorization/requirement for release, any applicable exceptions and associated documentation, communications with requesters, interim and final status of responses, any allegations of information blocking, and any enforcement actions for that request.

© 2022 The Sequoia Project. All rights reserved.

EHI Requests for Data in Archived Systems

- Good Practice: Review data on the nature, volume, and expected responses times (by patients) of prior PHI requests to help make decisions on what data to archive and when.

© 2022 The Sequoia Project. All rights reserved.

Individual Access Requests

- Good Practice: Provide patients with information on the EHI that is available to them and how they can access it consistent with the HIPAA right of access, information blocking regulatory requirements, state and other federal law, and the Actor organization's policies and procedures.
- Good Practice: Recognize and plan for the fact that a HIPAA-defined individual access request could come to the Actor, based on patient direction, from third party apps, legal counsel, etc., in addition to coming from the patient.
- Good Practice: Establish a centralized point of contact for an Actor's patients to request their EHI (recognizing that there may be other points of access, such as the patient's clinicians). This point of contact should use HIM and interoperability expertise within the organization.

© 2022 The Sequoia Project. All rights reserved.

Individual Access Requests

- Good Practice: Develop educational materials and programs (e.g., data-focused patient advocates), informed by equity and disparity reduction goals, to help patients understand EHI availability. These resources should also address the roles of Developers and HIEs/HINs as points of EHI access (especially in terms of what these Actors can and cannot do under BAAs and law and regulation)

- Good Practice: Recognize and address differences in how patients can access their EHI, including variations in computer, smart phone, and on-line opportunities; evaluate what "access" looks like for your population.

- Good Practice: Consistent with the type of Actor (e.g., HIE/HIN), identify, document, and communicate situations when a HIPAA authorization is required for EHI individual access or a direct request with patient authorization from an attorney or other party.

© 2022 The Sequoia Project. All rights reserved.

Interoperability MATTERS
an initiative of The Sequoia Project

Exceptions

© 2022 The Sequoia Project. All rights reserved.

Eight Exceptions are Identified by ONC

Not Fulfilling Requests to Access, Exchange, or Use EHI

1. Preventing Harm
2. Privacy
3. Security
4. Infeasibility
5. Health IT Performance

Procedures for Fulfilling Requests to Access, Exchange, or Use EHI

6. Content and Manner
7. Fees
8. Licensing

© 2022 The Sequoia Project. All rights reserved.

Using Exceptions: General

- Good Practice: For all exceptions that involve *not fulfilling* requests to access, exchange, or use EHI as requested, Actors should notify the requester promptly about the status of their request, why it cannot be met in whole or in part, and which exceptions apply. They should then document this response.
  - In responding to such requests, Actors should seek to adopt a culture of “yes if” rather than “no with documentation”.

© 2022 The Sequoia Project. All rights reserved.

Using Exceptions: General

- Good Practice: Recognize and plan for the use of multiple exceptions in some instances, sometimes sequentially (e.g., Content and Manner before Infeasibility) and in other instances in a more parallel fashion.
  - For example, there may be scenarios (e.g., those that involve state privacy laws on release of sensitive results where functions to support information blocking compliance are not available in an EHR), where it might be appropriate to use a combination of Privacy, Content and Manner, and Infeasibility at the same time.
  - Similarly, multiple exceptions may be needed (e.g., Privacy, Security, Content and Manner, and Infeasibility) where an Actor does not have a direct relationship with the individual requesting EHI access nor a portal that can provide the requested information. A similar scenario could arise with provision of EHI to adolescents where the Actor has knowledge or a reasonable belief that the parents are accessing the adolescent's portal account.
  - Another example is where a data outage leads to use of both Health IT Performance and Infeasibility.
  - Actors should develop **notification and documentation forms** for common multiple exception scenarios applicable to their experience. They should document especially the interacting circumstances that justify the need for multiple exceptions and any sequencing used to arrive at the final set of exceptions (e.g., Content and Manner and then Infeasibility).

© 2022 The Sequoia Project. All rights reserved.

Preventing Harm Exception

- Good Practice: In seeking to use this exception, the Actor should ensure and document that: (1) its practices for which this exception is to be used are “reasonable and necessary” to prevent harm to a patient or another person; (2) that they have a reasonable belief that the practice will substantially reduce the likelihood of harm to the patient or another person; and (3) that the practice is no broader than necessary to substantially reduce the risk of harm that the practice is implemented to reduce.

- Good Practice: Ensure that the organization’s policies enabling use of this exception align with the HIPAA Privacy Rule (i.e., that the type of harm being prevented is harm that a HIPAA covered entity could use to deny access to an individual’s PHI under the Privacy Rule’s Right of Access (45 CFR 162.524 (a)(3))).

© 2022 The Sequoia Project. All rights reserved.

Preventing Harm Exception

- Good Practice: Establish, train to, and document compliance with policies and procedures that ensure that the appropriate standard for denial of requested access, exchange, or use of EHI (e.g., "reasonably likely to endanger life or physical safety" or "reasonably likely to cause substantial harm to another person") is aligned with who is making the request (e.g., the patient, individual's legal representative, a provider or other party subject to the fourth condition of the exception), and who could be harmed (e.g., the patient, another party mentioned in the EHI).
  - It is especially important to recognize and use the higher bar of "endanger life or physical safety" when it is applicable (e.g., a patient request for their own information).
  - It is also important to recognize that the HIPAA "substantial harm" standard used by ONC includes "*substantial physical, emotional, or psychological harm". See* https://www.healthit.gov/curesrule/faq/which-patient-access-cases-does-preventing-harm-exception-recognize-substantial-harm and https://www.federalregister.gov/d/00-32678/p-1091.

© 2022 The Sequoia Project. All rights reserved.

Preventing Harm Exception

- Good Practice: If the request is from the patient's legal representative (including but not limited to personal representatives recognized at 45 CFR 164.502) or involves the patient's or their legal representative's access to, use or exchange of information that references another person:
  - ensure and document that the use of the exception is determined on an **individualized basis** in the **exercise of professional judgment** by a **licensed health care professional** who has a **current or prior clinician-patient relationship with the patient** whose EHI is affected by the determination; *or*
  - that it is due to data known or reasonably suspected to be misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason.

© 2022 The Sequoia Project. All rights reserved.

Preventing Harm Exception

- Good Practice: Establish and monitor uses of the Preventing Harm exception to ensure that all applicable criteria (e.g., **licensed healthcare professional who has a current or prior clinician-patient relationship** with the patient) are met.
  - Note: The fact that ONC states that use of this exception must be based on a "[p]ractice implemented based on an organizational policy or a determination specific to the facts and circumstances" does not obviate the requirement in other conditions of this exception to apply "individualized professional judgement" (e.g., as opposed to blanket policies that do not reflect such individualized professional judgement). ONC has stated in an FAQ that "blanket delays" for test results are inconsistent with the requirement for an individualized assessment.
  - Note: Licensed health care professionals who generate test results but do not have a prior clinician-patient relationship with the patient would generally be unable to use this exception when individualized professional judgement (as defined in the rule) is required.

© 2022 The Sequoia Project. All rights reserved.

Preventing Harm Exception

- Good Practice: Where the risk of harm is based on individualized professional judgement, implement the practice in a manner consistent with any rights the patient whose EHI is affected may have under § 164.524(a)(4) of the Code of Federal Regulations (Right of Individual Access), or any Federal, State, or tribal law, to have the determination reviewed and potentially reversed.

- Good Practice: Establish organizational criteria for determining that data is known or reasonably suspected to be misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason.

© 2022 The Sequoia Project. All rights reserved.

Preventing Harm Exception

- Good Practice: Create and train staff to organizational policies for the use of this exception that are **written**; based on relevant clinical, technical and other appropriate **expertise**; and implemented in a **consistent and non-discriminatory** manner.
  - Document that (and how) these policies are applied when used.

- Good Practice: Establish policies and procedures for making **individualized determinations of harm** (not necessarily the same as individualized professional judgement, which must be used even where a policy applies) based on **facts/circumstances** known or reasonably believed at the time of their use and with relevant expertise when the otherwise applicable organizational policies cannot be used.
  - Document when and how these determinations are made and establish an audit function for their use.

© 2022 The Sequoia Project. All rights reserved.

Privacy Exception

- Good Practice: When considering use of the Privacy exception, do not over-interpret HIPAA or other consent requirements or have patients opt out of sharing by default; ensure that organizational policies align with the information blocking rule as well as state and federal legal requirements.
- Good Practice: Be mindful of the role of **intent** in information blocking enforcement and reflect compliant intent in policies, procedures, and documented actions.
- Good Practice: Ensure that use of this exception reflects the fact that "individual" is defined more broadly than in HIPAA, to include others who have the legal authority to act on behalf of a patient under state or federal law.
- Good Practice – Ensure that the Actor meets **all** the elements of **at least one** sub-exception to claim this exception.

© 2022 The Sequoia Project. All rights reserved.

Privacy Exception

- Good Practice: Given the importance of documented policies and procedures for effective use of this exception, ensure that the Actor organization has privacy policies that reflect HIPAA and other applicable federal and state laws. (Note: some HIEs/HINs and Developers may only have HIPAA security policies but not HIPAA privacy policies.)

- Good Practice: Ensure, through training and documented policies and procedures, that the Actor's staff recognize that the information blocking regulation may require Actors to provide access, exchange, or use of EHI in situations where HIPAA **would not require** access to similar information (e.g., the HIPAA Privacy Rule **permits, but does not require**, covered entities to disclose ePHI in most situations).

© 2022 The Sequoia Project. All rights reserved.

Privacy Exception

- Good Practice: Establish a centralized process and organizational accountability (e.g., the unit responsible for EHR data access and/or internal HIPAA/privacy audits) for regular internal audits on the use of this and other exceptions, including frequency of use. Ensure that these audits address all potential access points for EHI requests where this exception might be used.
- Good Practice: To the greatest extent possible, centralize use of (or at least overall responsibility for) this exception and associated documentation within the Actor organization.
- Good Practice: Treat similar organizations and situations consistently, with documentation of any inconsistent practices or practices that do not comply with a documented organizational policy.
- Good Practice: If access to EHI is limited under this exception for a reason that is time-related (e.g., acquisition of a valid consent), provide a “window of estimated availability” for the requested EHI.

© 2022 The Sequoia Project. All rights reserved.

Privacy Exception

- Good Practice: sub-exception #1 – Precondition not satisfied:
  - If used, document the specific law(s) and regulation(s) that require the precondition being asserted (e.g., HIPAA, 42 CFR Part 2, state law or regulation).
  - Ensure that privacy-protective practices used for this sub-exception are based on **objective criteria**, **applied uniformly** for **all substantially similar** privacy risks.
  - **Tailor privacy protective practices** to the specific privacy risk and associated pre-condition (e.g., requirement for identity verification).
  - Except for an **individual's access** to their own EHI, Actors operating in multiple states should determine if it is feasible and desirable to use the regulatory ability to rely for this sub-exception on **documented** organizational policies and procedures that adopt the **more restrictive state** (and applicable Federal) **law** for the entire organization. Note that such a uniform approach is unavailable if a **case-by-case** approach to applying this sub-exception is used rather than a formal policy.

© 2022 The Sequoia Project. All rights reserved.

Privacy Exception

- Good Practice: sub-exception #2– Health IT developer not covered by HIPAA:
  - If claiming this exception, document that the health IT developer is not covered by HIPAA as a Covered Entity or Business Associate of a Covered Entity (e.g., health IT developer of certified health IT is involved in only direct-to-consumer products or services).
  - Ensure that privacy-protective practices used for this sub-exception are described in detail in the Actor's privacy policy and disclosed in advance to patients and others in plain language.
  - **Tailor** privacy protective practices to the specific privacy risk and associated pre-condition (e.g., requirement for identity verification).

© 2022 The Sequoia Project. All rights reserved.

Privacy Exception

- Good Practice: sub-exception #3 – Patient right of access:
  - If used, ensure that practices are limited to the "unreviewable" grounds for denying access to PHI under the HIPAA Privacy Rule (e.g., the request is for psychotherapy notes, or information compiled in reasonable anticipation of, or for use in, a legal proceeding).
- Note: "reviewable" grounds under HIPAA are covered by the Preventing Harm exception.

© 2022 The Sequoia Project. All rights reserved.

Privacy Exception

- Good Practice: sub-exception #4 – Respecting an individual's request to not share information:
  - If used, document that the request to not share information comes from the individual whose PHI it is.
  - Implement use of this exception in a **consistent, non-discriminatory** manner as documented in organizational policies and procedures.
  - Ensure and document that there was **no interference or pressure** on the individual who made the request not to share.

© 2022 The Sequoia Project. All rights reserved.

Security Exception

- Good Practice: An Actor that may wish to use this exception should have or develop a written organizational security policy that is (1) prepared for or directly responsive to security risks identified by the Actor; (2) aligned with consensus-based standards/best practices (e.g., as identified by the HHS Office of Civil Rights, NIST, and/or ONC); and (3) that provides objective timeframes/other parameters for identifying, responding to and addressing security incidents:
  - This policy and associated procedures and technologies should be appropriate to and scaled for the organization's Actor-type, size and structure and risks to individuals' EHI. The Actor should also have a process to identify practices that exceed HIPAA (which may not be straightforward given how the HIPAA Security Rule is designed). There should be a documented rationale for any security practices that exceed minimum HIPAA Security conditions (e.g., required of a Developer or HIE/HIN in a Business Associate Agreement, an agreement with an HIE or an interoperability framework, or a documented internal security review).
  - The review and update of the Actor's security policy should take place well in advance of any likely need for use of the Security exception.
  - Identify and document specific industry standards used in the security policy.

© 2022 The Sequoia Project. All rights reserved.

Security Exception

- Good Practice: An Actor that wishes to use this exception should ensure that security-related practices **likely to interfere with access, exchange or use of EHI** are documented as meeting the following criteria:
  - Directly related to safeguarding confidentiality, integrity, and availability of EHI;
  - Tailored to the specific security risks being addressed;
  - Implemented in a consistent and non-discriminatory manner;
  - If implementing an existing organizational security policy, that fact is documented;
  - Security practices that exceed minimum HIPAA Security conditions should have a documented rationale; and
  - If the practice is not implementing an organizational security policy, ensure and document that the practice is based on specific facts and circumstances that make it necessary to mitigate risks and there is no reasonable alternative.

© 2022 The Sequoia Project. All rights reserved.

Security Exception

- Good Practice: Recognize that ONC takes the view that, for third-party apps chosen by individuals to facilitate their access to their EHI held by Actors, there would generally not be a need for "vetting" on security grounds, other than for the impact on the Actor's own EHI security. Actors do, however, have the ability to conduct whatever 'vetting' they deem necessary of entities (e.g., app developers) that would be their HIPAA business associates.

- Good Practice: As appropriate, build organizational processes and templates that support multiple exceptions, including the Security exception.
  - One example could be an Infeasibility determination document that includes the Security documentation for why an EHI request cannot be fulfilled because a certain level of security has not been met (e.g., identity verification) **and** the resources do not exist to create the technical or administrative processes to facilitate that access.
  - Similarly, indicate to data requesters if the **manner** of the EHI request raises certain Security concerns that might not be raised by an Alternate Manner for the Content and Manner exception.

© 2022 The Sequoia Project. All rights reserved.

Infeasibility Exception

- Good Practice: Establish policies, procedures, documentation, and training to enable use of this exception to decline to provide access, exchange, or use of EHI in a manner that is **infeasible**, carefully reviewing and adapting its three distinct conditions for infeasibility and recognizing that ONC intends for this exception to be a **high bar**:
  1. The Actor cannot fulfill the request for access, exchange, or use of EHI due to events **beyond the Actor's control**, namely a natural or human-made disaster, public health emergency, public safety incident, war, terrorist attack, civil insurrection, strike or other labor unrest, telecommunication or internet service interruption, or act of military, civil or regulatory authority;
  2. The Actor cannot **unambiguously segment** requested EHI from other EHI; or
  3. **Infeasible under the circumstances** as demonstrated by **contemporaneous documentation**, **consistent and non-discriminatory** consideration of several factors including the Content and Manner exception and whether the Actor's practice is **non-discriminatory** and the Actor provides the same access, exchange, or use of EHI to its companies or to its customers, suppliers, partners, and other persons with whom it has a business relationship.

© 2022 The Sequoia Project. All rights reserved.

Infeasibility Exception

- Good Practice: In general, an Actor should work through the Content and Manner exception before using the Infeasibility exception, especially the "Infeasible under the Circumstances" conditions for which the Actor must explain why it did not use the Content and Manner exception.

- Good Practice: If there is an anticipated need to use the Infeasibility exception, work through the Content and Manner exception on a timetable that will allow timely assertion of the Infeasibility exception (i.e., within ten business days of receipt of the original request for EHI, provide to the requestor in writing the reason(s) why the request is infeasible). In addressing this timing requirement, the Actor should **document its good faith effort to use Content and Manner** so that this information on intent can be considered by enforcement authorities evaluating the facts and circumstances of a potential information blocking complaint.

© 2022 The Sequoia Project. All rights reserved.

Infeasibility Exception

- Good Practice: Create processes to track receipt of non-routine or other EHI requests that might require the Infeasibility exception and to enable response to infeasible requests within ten business days of receipt of the request:
  - This timing may be affected by initial, failed efforts to use the Content and Manner exception, which may make the Infeasibility exception unavailable. In this scenario, ONC has taken the position that a **case-by-case analysis** of an information blocking allegation would consider the **documented effort** to use the Content and Manner exception.
  - If the initial communication from the requester does not have a sufficient basis to determine what the request is or to begin an assessment of its feasibility, document that fact and the time needed to finish the initial due diligence needed to **begin** an infeasibility assessment. ONC has indicated orally that such due diligence should not count against the 10-business day infeasibility review.
  - Prepare, if the Content and Manner exception is being pursued, a **draft notification of infeasibility**, consistent with the conditions of the Infeasibility exception, that could be provided timely if Content and Manner cannot ultimately be used.
  - Ensure that the timing of responses is **not discriminatory** regarding specific types of requesters, especially competitors.

© 2022 The Sequoia Project. All rights reserved.

Infeasibility Exception

- Good Practice: Establish policies, procedures, documentation, and training to enable use of the **first condition** of this exception, that the Actor cannot fulfill the request for access, exchange, or use of EHI due to **events beyond the Actor's control** (e.g., a natural or human-made disaster, public health emergency, public safety incident, war, terrorist attack, civil insurrection, strike or other labor unrest, telecommunication or internet service interruption, or act of military, civil or regulatory authority).
  - Document the nature of the eligible events and how they made responding to a request to be infeasible.
  - To enable meeting the 10-day notification requirements for this condition, plan for notification approaches that might make such timing more feasible, such as a banner or other information on the Actor's website or portal providing general notice of EHI unavailability given the circumstances that underlie the use of this first condition of the Infeasibility exception.

© 2022 The Sequoia Project. All rights reserved.

Infeasibility Exception

- Good Practice: Establish policies, procedures, documentation, and training to enable use of the **second condition** of this exception, that the Actor **cannot unambiguously segment** requested EHI from other EHI that (1) cannot be made available due to an individual's preference or because the EHI cannot, by law, be made available; or (2) may be withheld in accordance with the Preventing Harm exception.
  - Document the capabilities and limitations on data segmentation in the Actor's EHR and other applicable HIT as well as in the Actor's workflow, including the ability to use data segmentation standards such as those in ONC certification criteria (§170.315(b)(7) - Security tags - summary of care – send, which uses the HL7 Data Segmentation for Privacy standard); and
  - Document the specific segmentation that would be needed to meet a documented sub-condition 1 or 2 and why such segmentation cannot be accomplished.

© 2022 The Sequoia Project. All rights reserved.

Infeasibility Exception

- Good Practice: Establish policies, procedures, documentation, and training to enable use of the **third condition** of this exception, that responding favorably to the request is **infeasible under the circumstances** as demonstrated by **contemporaneous documentation, consistent and non-discriminatory** consideration of several factors including:
  - the type of EHI and the purposes for which it may be needed;
  - the cost of complying with the request in the manner requested;
  - financial and technical resources available to the Actor (e.g., could include the need to make decisions on where to invest to enable EHI availability);
  - whether the practice is non-discriminatory and whether the Actor provides the same access, exchange, or use of EHI to its companies 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, HIE, or HIN through which EHI is accessed or exchanged; and
  - why the Actor could not provide access, exchange, or use of EHI consistent with the EHI Information Content and Manner exception.
  - Note: In determining if the circumstances were infeasible, do not factor in whether the manner requested would have facilitated competition with the Actor or prevented the Actor from charging a fee or resulted in a lower fee and ensure that documentation reflects that these factors played no role in determining infeasibility.

© 2022 The Sequoia Project. All rights reserved.

Health IT Performance Exception

- Good Practice: Document how a practice for which this exception is claimed is intended to maintain or improve health IT performance.

- Good Practice: For maintenance or improvements to health IT that make the health IT temporarily unavailable or temporarily degraded, ensure and document that the interruption lasts **no longer than necessary** and is implemented in a **fair and consistent** manner.

© 2022 The Sequoia Project. All rights reserved.

Health IT Performance Exception

- Good Practice: Actions taken by an Actor with third-party applications (including but not limited to patient-facing apps) that are negatively affecting the Actor's health IT performance should be taken for **no longer than necessary** to resolve any negative impacts, implemented in a **consistent and non-discriminatory manner**, and be **consistent with existing SLAs**, where applicable.

- Good Practice: Establish, implement, and train staff on policies that ensure that performance degradations that could limit access, exchange, or use of EHI **and that also fall within the scope of the Harm or Security exceptions meet those exceptions**; these need not also meet the HIT Performance exception.

© 2022 The Sequoia Project. All rights reserved.

Health IT Performance Exception

- Good Practice: For Developers and HIEs/HINs
  - Create or revise Service Level Agreements (SLAs) with parties that rely on or expect regular access, exchange, or use of EHI to allow for both “planned” and “unplanned” interruptions. Document that such interruptions are both consistent with the SLA(s) and **no longer than necessary** even if a longer interruption would be consistent with the SLA.
  - An Actor organization that does not have SLAs in place with date requesters who will expect uninterrupted service should develop such SLAs and routinely include them as an exhibit to the service agreement.
  - Prospectively account for unplanned/unavoidable downtimes in SLAs. These are often reflected in SLAs as excluded events and including them in the SLA can document data requester acknowledgment of such potential circumstances and that it is not always possible to get permission in advance.
  - If unplanned interruptions are not consistent with existing SLAs, ensure and document that the interruptions have been agreed to by the applicable data requester(s). If such agreement is not feasible, document why it is not, to support potential **facts and circumstances** review by enforcement agencies.
  - Note: Although Provider Actors need not rely on SLAs for interruptions, they might need their own SLA provisions if they are sublicensing a vendor technology to end users (e.g., patient portal, third-party provider portals, payer portals, etc.).

© 2022 The Sequoia Project. All rights reserved.

Content and Manner Exception

- Good Practice: Use this exception as an initial “gateway” to decisions on using certain other exceptions in the information blocking regulations, especially Infeasibility, Fees, and Licensing (responding to a request for EHI in the manner requested can obviate the need to use the Fees and Licensing exceptions).

- Good Practice: Recognize that this exception focuses on the **manner** in which a request for EHI is handled; ONC emphasizes that the **content** to be provided has no optionality. The Actor must provide all EHI that is requested and may be legally provided to the requester so long as no other exception applies. Note further that responses to EHI requests that involve EHI duplicated in multiple Actor HIT systems or locations could be viewed as provision in an **alternative manner** if a different location is offered than that cited in the EHI request.

© 2022 The Sequoia Project. All rights reserved.

Content and Manner Exception

- Good Practice: In general, an Actor should work through the Content and Manner exception before using the Infeasibility exception, especially the **Infeasible under the Circumstances** conditions for which the Actor must explain why it did not use the Content and Manner exception.

- Good Practice: In using Content and Manner, if there is an anticipated need to use the Infeasibility exception, make every effort to work through the conditions and manner hierarchies in the Content and Manner exception on a timetable that will allow timely assertion of the Infeasibility exception (i.e., within ten business days of receipt of the original request for EHI, provide to the requestor in writing the reason(s) why the request is infeasible). In addressing this timing and notification requirement, the Actor should:
  - Document its good faith effort to use Content and Manner so that this information on intent can be considered by enforcement authorities evaluating the **facts and circumstances** of a potential information blocking complaint.
  - Prepare, **while the Content and Manner exception is being pursued**, a draft notification of infeasibility, consistent with the conditions of the Infeasibility exception that could be provided timely if Content and Manner cannot ultimately be used.

© 2022 The Sequoia Project. All rights reserved.

Content and Manner Exception

- Good Practice: Given the costs associated with applying the Content and Manner and Infeasibility exceptions (e.g., development of processes, staff time to work through Content and Manner issues and to develop Infeasibility notifications, data requester unhappiness, etc.), actors should evaluate the potential for reductions in such costs in weighing investment decisions (whether and when) to acquire or implement new technology that could reduce the need for using these exceptions.

© 2022 The Sequoia Project. All rights reserved.

Content and Manner Exception

- Good Practice: Recognize that an Actor must fulfill a request for EHI in **any manner requested**, unless the Actor is technically unable to comply, or the Actor cannot reach terms with requestor. Document technical inability or **inability to reach terms**, emphasizing evidence of a good faith effort to provide the EHI in the manner requested.

- Good Practice: Recognize that, in implementing this exception, ONC defines **technically unable** as meaning the Actor cannot comply due to technical limitations with its systems (e.g., request is for API access and the Actor cannot use an API). ONC stresses this condition is a **very high bar** and does not include an Actor's "preference" to fulfill differently due to cost, burden or similar reason.
  - Note: ONC does not require Actors to implement or upgrade specific technologies, standards or capabilities (e.g., certified health IT) per ONC FAQs. https://www.healthit.gov/curesrule/faq/do-information-blocking-regulations-require-actors-have-or-use-certified-health-it-or-upgrade, https://www.healthit.gov/curesrule/faq/how-actor-expected-fulfill-request-for-uscdi-under-content-and-manner-exception-if-they-do-not, and https://www.healthit.gov/curesrule/faq/for-period-time-when-information-blocking-limited-united-states-core-data-for-interoperability

© 2022 The Sequoia Project. All rights reserved.

Content and Manner Exception

- Good Practice: Actors using this exception should (1) document that a request under this exception is handled in “any” or an “alternative” manner requested; (2) document/catalog areas of technical infeasibility and prepare, **in advance**, communications regarding these areas of infeasibility; (and 3) develop and update over time internal statements of intent regarding the Actor’s ongoing consideration of additions to the “menu” of available alternative manners.

- Good Practice: Consider using existing or new mechanisms (e.g., websites announcing product or service updates or providing documentation) that enable data requesters to subscribe or check for new information on **updated content and manner options**, including options that would enable fulfillment of an earlier request.

© 2022 The Sequoia Project. All rights reserved.

Content and Manner Exception

- Good Practice: In using this exception, and the **Any Manner Requested** condition to avoid use of the Fees and/or Licensing exceptions, establish and train staff for policies and procedures that both reflect ONC regulatory requirements for “any manner” and also the potential benefits of using “any manner,” especially for non-routine EHI requests.

- Good Practice: Recognize that inability to come to terms with a requester (e.g., inability to agree on fees or other commercial terms) provides a basis to seek to proceed from to an **Alternative Manner** in this exception.

© 2022 The Sequoia Project. All rights reserved.

Content and Manner Exception

- Good Practice: Create, and train staff to, policies and procedures for the expected common situations where the Actor cannot fulfill an EHI request in “any manner requested”.

- Good Practice: Consider centralized responsibility for this exception, or at least a central point for expertise and for **auditing of exception use**.

© 2022 The Sequoia Project. All rights reserved.

Content and Manner Exception

- Good Practice: Policies and procedures for this exception should follow the ONC hierarchy of potential "alternate manner" responses, being mindful of requirements and definitions in the regulation and its preamble, as well as ONC FAQs.

- Good Practice: The Actor should work through the hierarchy of possible "alternative manner" responses in the order specified by ONC "without unnecessary delay," only moving to a next level approach if the prior level could not be used. The Actor should document progress through the hierarchy, the appropriateness of response timing, the reasons for any timing that could be perceived as a delay, and any reasonable "skipping ahead" in the sequence of approaches (e.g., client request).

© 2022 The Sequoia Project. All rights reserved.

Content and Manner Exception

- Good Practice: To use the **first level** of "alternative manners," the Actor should document, in advance of any requests, the availability of technologies certified to standard(s) adopted in ONC certification rules that could be used to meet EHI requests. The Actor should then document whether use of such standards was specified by requestor and whether the Actor was able to use this technology to meet the EHI request or why they were not able to do so.

- Good Practice: To use the **second level** of "alternative manners," the Actor should document, in advance of any requests, the availability for use by the Actor of content and transport standards specified by the requestor and published by the Federal Government (e.g., in a regulation issue by CMS or ONC) or an ANSI accredited standards development organization (e.g., HL7, DirectTrust) that could be used to meet EHI requests. The Actor should then document whether the use of such standards was specified by requestor and whether the Actor was able to use this technology to meet the EHI request or why they were not able to do so.

© 2022 The Sequoia Project. All rights reserved.

Content and Manner Exception

- Good Practice: To use the **third level** of "alternate manners," the Actor should document, in advance of any requests, the availability of machine-readable formats (and the means to interpret the EHI, such as a data schema) that could be used to meet EHI requests. The Actor should then document whether the use of such formats was agreed to by the requestor and whether the Actor was able to use these formats to meet the EHI request or why they were not able to do so.
  - Note: ONC has stated in an FAQ that a PDF document could meet this criterion if it meets the National Institute of Standards and Technology's definition of machine-readable – " Product output that is in a structured format, typically XML, which can be consumed by another program using consistent processing logic." "If a data output format is structured so that the EHI it conveys is machine readable, then that output format is a machine-readable format, regardless of the file extension." As ONC notes, PDFs that are or contain images (as opposed to fully editable text) may not meet the definition of machine readable. A key consideration is that use of this third "alternate manner" for PDFs must be "mutually agreeable," meeting the specific needs of the requester.

© 2022 The Sequoia Project. All rights reserved.

Fees Exception

- Note: This exception is relevant for all Actors, but its frequency and nature of use will vary across and within Actor categories.
  - Developers and HIEs/HINs will need to determine when a fee and when a license apply and use the applicable exception.
  - Providers, like other Actors, would use this exception whenever they charge a fee for an interoperability element used for access, exchange, or use of EHI.
    - For example, although the HIPAA Privacy Rule prohibits fees for responding to certain types of patient data requests (e.g., access to PHI available through certified EHR technology), it does allow such fees in other cases. Sometimes these fees are restricted (e.g., labor for copying the PHI requested by the individual in electronic form) and sometimes they are not restricted (e.g., where a third party is initiating a request for PHI on its own behalf, with the individual's HIPAA authorization). All such fees would generally be subject to the Fees exception.

© 2022 The Sequoia Project. All rights reserved.

Fees Exception

- Good Practice: Train team members to understand that, while charging a fee to fulfill a request for EHI is not prohibited by the information blocking rule, such fees can implicate information blocking and generally must be used in conjunction with the Fees exception, which applies to fees charged by all Actor-types.
  - Team members to be trained are those involved in setting, negotiating, or reviewing fees for interoperability elements (e.g., commercial and pricing teams, legal, finance, field engineers installing interfaces, etc., and Business Associates and agents with these functions).

- Good Practice: Plan for situations when use of the **Any Manner Requested** path in the Content and Manner exception enables the Actor to avoid the Fees exception, especially for fees for non-routine EHI requests.

- Good Practice: Develop and implement procedures to use the Fees exception for fees associated with EHI licensing that are other than royalties permitted and addressed under the Licensing exception.

© 2022 The Sequoia Project. All rights reserved.

Fees Exception

- Good Practice: Developers of certified Health IT wishing to use this exception should also ensure that they are compliant with the **Conditions of Certification** in 170.402(a)(4), 170.404, or both for all practices and at all relevant times.

- Good Practice: Establish processes, procedures and staff/organizational accountability to implement the Fees exception, including estimating and allocating needed time and resources for initial and additional ongoing review of new and existing contracts and prices.

© 2022 The Sequoia Project. All rights reserved.

Fees Exception

- Good Practice: Work with the Actor's finance and commercial teams to ensure and document that profit margins associated with current and future fees for EHI access, exchange, or use could be defended as **reasonable** given comparable industry data and as part of an enforcement agency consideration of the applicable **facts and circumstances**.

- Good Practice: Work with the Actor's finance and commercial teams to ensure and document that any current and future fees are:
  - based on objective and verifiable criteria uniformly applied to all similarly situated persons/ requests;
  - reasonably related to the costs of providing access, exchange, or use;
  - reasonably allocated among all similarly situated persons or entities that use the product/service (intended to allow approaches like sliding fee scales per comments on the Proposed Rule); and
  - based on costs not otherwise recovered for the same instance of service to a provider and third party.
  - **Note: The granularity of the data analysis to support these analyses, which could be very burdensome, should reflect the Actor's size, scale, complexity, and resources, with the rationale for methods used and not used documented.**

© 2022 The Sequoia Project. All rights reserved.

Fees Exception

- Good Practice: Use the following list of prohibited bases for fees for EHI access, exchange, or use as a checklist for initial and ongoing review by the Actor's finance and commercial teams, ensuring that fees are not based:
  - ✓ in any part on whether requestor is a competitor, potential competitor, or will be using EHI to facilitate competition with the Actor;
  - ✓ on sales, profit, revenue, or other value the requestor derives or may derive, that exceed the Actor's reasonable costs (e.g., as a percent of sales revenue);
  - ✓ on costs that led to creation of intellectual property (IP), if the Actor charged a royalty for that IP per the Licensing exception and the royalty was included in development costs for IP creation;
  - ✓ on costs the Actor incurred due to the health IT being designed or implemented in a non-standard way, unless the requestor agreed to fees associated with non-standard approach (document that the approach used available standards appropriate to the request;
  - ✓ on costs associated with intangible assets other than actual development or acquisition costs;
  - ✓ on opportunity costs unrelated to access, exchange, or use of EHI;

© 2022 The Sequoia Project. All rights reserved.

Fees Exception

- Good Practice: Use the following list of prohibited bases for fees for EHI access, exchange, or use as a checklist for initial and ongoing review by the Actor's finance and commercial teams, ensuring that fees are not based (continued):
  - ✓ on anti-competitive or other impermissible criteria; or
  - ✓ on costs associated with:
    - ✓ **EHI export using ONC certified EHI export capabilities** (170.315(b)(10)) to enable switching health IT or to provide patients their EHI; export or data conversion from an EHR technology that was not agreed to in writing at the time the technology was acquired,
    - ✓ **electronic access by individuals to their EHI**
      - – Note: "electronic access" is defined by ONC as an "internet-based method that makes EHI available at the time the EHI is requested and where **no manual effort** is required to fulfill the request ".
    - ✓ **fees prohibited by the HIPAA Privacy Rule**—Access of individuals to protected health information - 45 CFR 164.524(c)(4).
      - ✓ For example, fees that exceed costs associated with specified labor, supplies, postage, summary preparation.

© 2022 The Sequoia Project. All rights reserved.

Fees Exception

- Good Practice: Review standard fees and data use agreements to ensure that they meet the requirements of the Fees exception.
- Good Practice: Template agreements and fee schedules that involve access, exchange or use of EHI should be designed to meet Fees and Licensing exception conditions.
  - Use of the Infeasibility exception should support decisions not to use the Content and Manner exception, for example, for a custom build sought by a data requester.
- Good Practice: If using the Fees exception, for example due to lack of agreement on **Any Manner Requested** in the Content and Manner exception, document why this exception is being used.
  - For example, Developers may have standardized fees as a matter of efficiency and using these fees and the Fees exception, rather than “Any Manner Requested” may be most appropriate.

© 2022 The Sequoia Project. All rights reserved.

Fees Exception

- Good Practice: When using the Fees exception, provide data requesters transparency in how fees were established and how they meet the requirements of the exception.
  - Note: Recognize that fees can meet the conditions of the exception and still be unaffordable to a particular requester and potentially generate complaints of information blocking.

- Good Practice: Review the definition of interoperability elements in the ONC Information Blocking Final Rule and determine how this definition applies to an Actor's technologies and services in the context of the potential need for, use of, and scope of the need for the Fees exception.

© 2022 The Sequoia Project. All rights reserved.

Licensing Exception

- Good Practice: Develop processes, procedures and accountability for implementing the Licensing exception, including estimating and allocating needed time and resources for initial and additional ongoing review of new and existing contracts.

- Good Practice: Establish policies and procedures to ensure that, for licenses subject to this exception, negotiations begin within 10 business days from receipt of a request and that the Actor negotiates, in good faith, a license within 30 business days from receipt.
  - Document receipt of licensing requests, the start of negotiations, facts that demonstrate the Actor's good faith, the timing in which negotiations are concluded, and the reason for any unavoidable delays that may hinder meeting these timelines. The latter could be important in enforcement agency facts and circumstances reviews.

© 2022 The Sequoia Project. All rights reserved.

Licensing Exception

- Good Practice: Identify all current and future licenses used by the Actor organization for ONC-defined interoperability elements.

- Good Practice: Review all identified licenses against the detailed criteria in the exception, focusing on such licensing conditions as:
  - scope of rights;
  - reasonable, non-discriminatory royalty and terms (e.g., an Actor may not charge a royalty for intellectual property (IP) if the Actor recovered any development costs that led to the creation of the IP using the Fees exception);
  - non-discriminatory terms (e.g., based on objective and verifiable criteria uniformly applied for all similarly situated classes of persons and requests and not based on competitive consideration or revenue or other value the requestor may derive from access, exchange, or use of EHI obtained via the interoperability elements).
  - prohibited collateral terms;
  - permitted non-disclosure agreement terms; and
  - additional conditions relating to provision of interoperability elements to prohibit impeding a licensee's efforts to use licensed elements.
  - **Note: The granularity of the data analysis to support these evaluations, which could be very burdensome, should reflect the Actor's size, scale, complexity, and resources. Make sure to document the rationale for methods used and not used.**

© 2022 The Sequoia Project. All rights reserved.

Licensing Exception

- Good Practice: Review the licensing practices in the information blocking proposed rule that ONC indicates could be information blocking as part of an internal analysis of licenses that might require an exception and/or changes in terms.

- Good Practice: Plan for situations when use of the **Any Manner Requested** path in the Content and Manner exception enables the Actor to avoid use of the Licensing exception, especially for licenses for non-routine licenses.

- Good Practice: Develop and implement procedures to use the Fees exception for fees associated with EHI licensing that are other than royalties permissible under the Licensing exception.

© 2022 The Sequoia Project. All rights reserved.

Licensing Exception

- Good Practice: Ensure that legal, contracting, and commercial teams recognize and plan for the fact that ONC expects Actors to take "immediate steps" to come into compliance with the Licensing exception by amending contracts or agreements to eliminate or void any clauses that are inconsistent with the provisions of this exception. The Actor should document the "immediate steps" taken, any needed timelines to complete the task and good faith rationales for this timing, and importantly, a process to "immediately" halt enforcement of any contract provisions that are inconsistent with the exception. See also an ONC FAQ on this point.

- Good Practice: Ensure that legal and contracting staff understand that an Actor **need not license all their intellectual property** (IP) or interoperability elements per this exception to a firm that requests a license **solely to develop its own technologies** and not to meet current needs for exchange, access or use of EHI to which it had a "claim" for specific patients or individual access.

© 2022 The Sequoia Project. All rights reserved.

Interoperability MATTERS
an initiative of The Sequoia Project

the sequoia project

Information Blocking Compliance Work Group

Contact Us

Thank you for your interest in Interoperability Matters and Information Blocking Compliance. If you would like to get in touch you can reach us at:

Interopmatters@sequoiaproject.org

© 2022 The Sequoia Project. All rights reserved.

Interoperability MATTERS
an initiative of The Sequoia Project

Appendix–Information Blocking Regulations and Compliance: Brief Overview

© 2022 The Sequoia Project. All rights reserved.

Understanding Information Blocking Compliance

- This Appendix provides a high-level overview of key information blocking compliance issues. Although it is intended to provide context for the Good Practices in this document, this report, including the Appendix, assumes that readers will have a detailed familiarity with information blocking compliance requirements applicable to their organization and professional roles.

- We encourage readers to also review the resources identified on page 120 and other available information, as appropriate, to guide more complete and detailed compliance and information sharing initiatives relevant to their organization and specific needs.

© 2022 The Sequoia Project. All rights reserved.

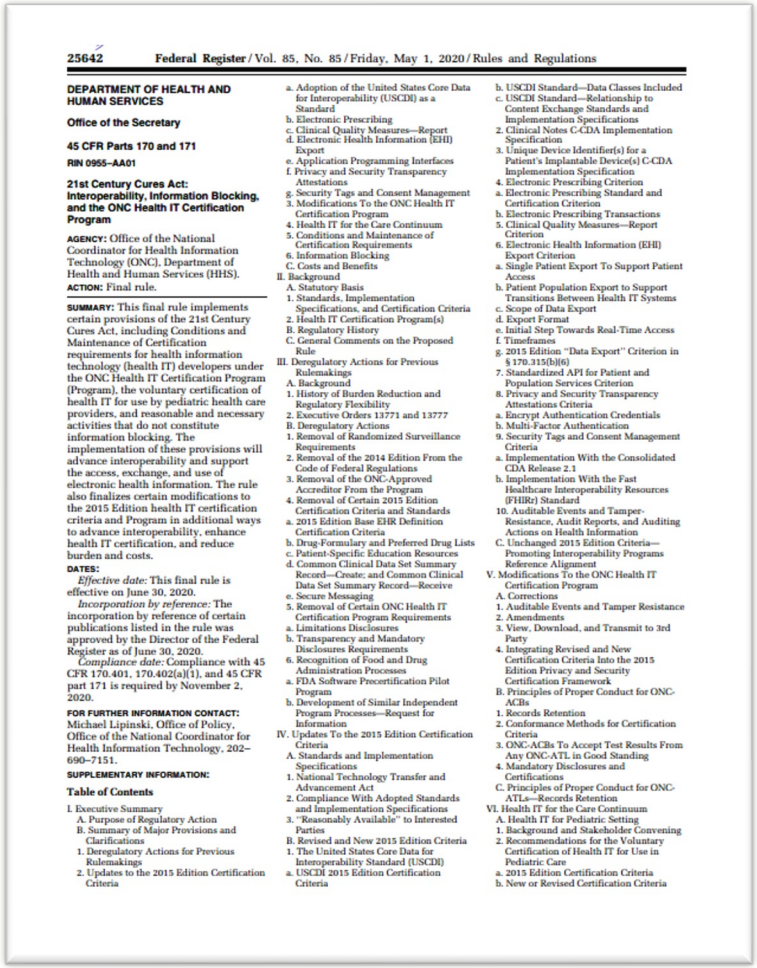
Information Blocking Compliance: An Urgent Matter for Healthcare Organizations

- In December 2016, Congress passed the 21st Century Cures Act (Cures), which prohibited **information blocking** and required actions to increase interoperability and information sharing.
- Cures defined "information blocking" as: **practices** that:
  - prevent or materially discourage **access, exchange or use of electronic health information** (EHI); and
  - for which the **Actor knows**, or [for some actors] **should know**, are **likely to interfere** with EHI **access, exchange, or use.**
- Cures also defined penalties for certain Actors (**up to $1 million per violation**) and required HHS (i.e., Office of the National Coordinator for Health IT—ONC) to issue implementing regulations.
- **The applicability date for the resulting ONC regulations was April 5, 2021, with enforcement dates to be determined by later HHS regulations.**

103
© 2022 The Sequoia Project. All rights reserved.

21st Century Cures and Interoperability: Regulations

- In March 2021, ONC issued a Final Rule implementing several Cures health IT provisions: *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program* (published in the *Federal Register* 5/1/2021) that:
  - builds on a March 2019 Proposed Rule,
  - addresses information blocking and certification relevant to interoperability, and
  - defines terms in Cures and sets the stage for enforcement.



25642 Federal Register / Vol. 85, No. 85 / Friday, May 1, 2020 / Rules and Regulations

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

45 CFR Parts 170 and 171

RIN 0955–AA01

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

AGENCY: Office of the National Coordinator for Health Information Technology (ONC), Department of Health and Human Services (HHS).

ACTION: Final rule.

SUMMARY: This final rule implements certain provisions of the 21st Century Cures Act, including Conditions and Maintenance of Certification requirements for health information technology (health IT) developers under the ONC Health IT Certification Program (Program), the voluntary certification of health IT for use by pediatric health care providers, and reasonable and necessary activities that do not constitute information blocking. The implementation of these provisions will advance interoperability and support the access, exchange, and use of electronic health information. The rule also finalizes certain modifications to the 2015 Edition health IT certification criteria and Program in additional ways to advance interoperability, enhance health IT certification, and reduce burden and costs.

DATES:

Effective date: This final rule is effective on June 30, 2020.

Incorporation by reference: The incorporation by reference of certain publications listed in the rule was approved by the Director of the Federal Register as of June 30, 2020.

Compliance date: Compliance with 45 CFR 170.401, 170.402(a)(1), and 45 CFR part 171 is required by November 2, 2020.

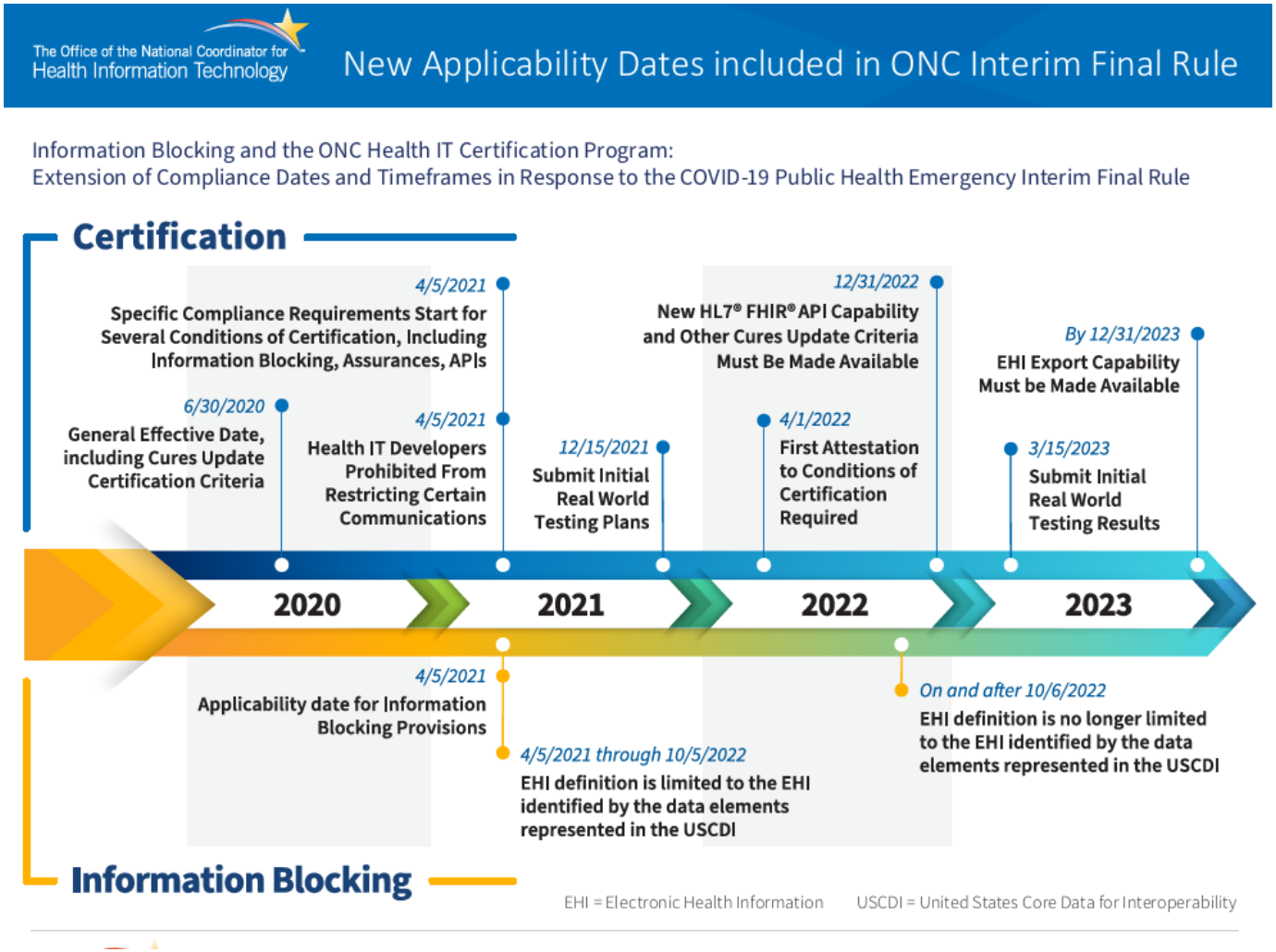
FOR FURTHER INFORMATION CONTACT: Michael Lipinski, Office of Policy, Office of the National Coordinator for Health Information Technology, 202–690–7151.

SUPPLEMENTARY INFORMATION:

Table of Contents

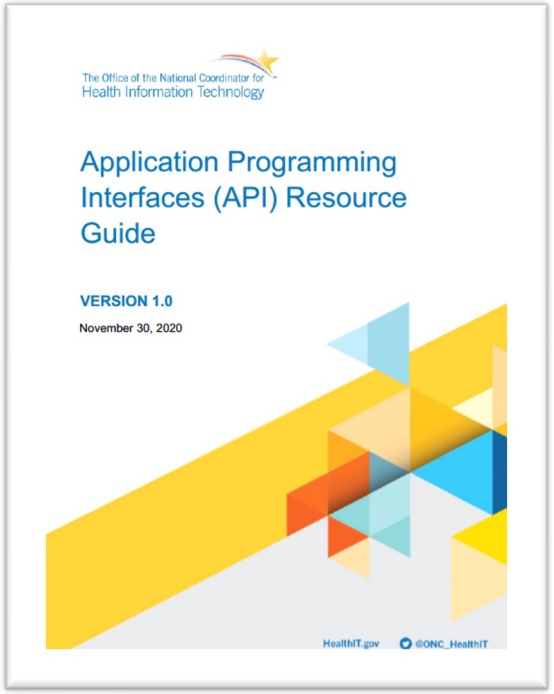
© 2022 The Sequoia Project. All rights reserved.

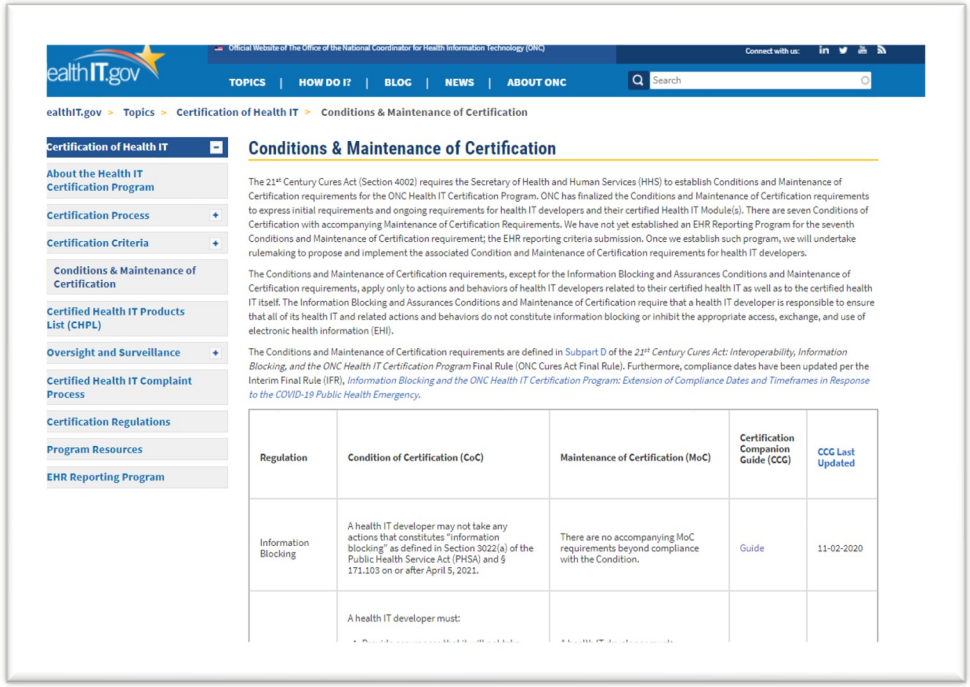
ONC Final Rule: Key Dates



© 2022 The Sequoia Project. All rights reserved.

The ONC Final Rule Also Establishes New Data Access Requirements for Developers of Certified Health IT, per Cures





ONC has published detailed technical certification resources relevant for developers and others.

© 2022 The Sequoia Project. All rights reserved.

How is Information Blocking Defined?

Information Blocking is a **practice** that—

Except as **required by law** or covered by an **exception**, is likely to **interfere with, prevent, or materially discourage access, exchange, or use** of **electronic health information**; **and**

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**

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**.

Highlighted terms are central to regulatory implementation. Note the “higher bar” for determining information blocking for Providers.

© 2022 The Sequoia Project. All rights reserved.

Eight Exceptions are Identified by ONC

Not Fulfilling Requests to Access, Exchange, or Use EHI

1. Preventing Harm
2. Privacy
3. Security
4. Infeasibility
5. Health IT Performance

Procedures for Fulfilling Requests to Access, Exchange, or Use EHI

6. Content and Manner
7. Fees
8. Licensing

 © 2022 The Sequoia Project. All rights reserved.

Who is Subject to Information Blocking Enforcement: "Actors" Are Defined by the ONC Regulations

- **Health Care Providers** – Extremely broad definition based on pre-existing definition in federal law (42 U.S.C. 300jj)
- **Health IT Developers of Certified Health IT** – Focus on those with ***any*** certified health IT (but enforcement is not limited to the certified health IT)
- **Health Information Network (HIN) or Health Information Exchange (HIE)** – Combined into one category in the ONC Final Rule; this is a ***functional definition*** that focuses on what the entity does, not how it is structured

© 2022 The Sequoia Project. All rights reserved.

Who Are the "Actors" Subject to Information Blocking Enforcement as Defined by ONC Regulation?

Health Care Providers	Same meaning as "health care provider" at 42 U.S.C. 300jj—this ***very broad definition*** includes 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, pharmacist, pharmacy, laboratory, physician, practitioner, provider operated by, or under contract with, the IHS or by an Indian tribe, tribal organization, or urban Indian organization, rural health clinic, a covered entity ambulatory surgical center, therapist, and any other category of health care facility, entity, practitioner, or clinician determined appropriate by the Secretary. ***Note: many of these categories will not have acquired ONC certified health IT.***

© 2022 The Sequoia Project. All rights reserved.

Who Are the "Actors" Subject to Information Blocking Enforcement as Defined by ONC Regulation?

Health IT Developers of Certified Health IT	An individual or entity, **other than a health care provider that self-develops health IT for its own use**, that **develops or offers** health information technology (as that term is defined in 42 U.S.C. 300jj(5)) and which has, at the time it engages in a practice that is the subject of an information blocking claim, one or more Health IT Modules certified under a program for the voluntary certification of health information technology that is kept or recognized by the National Coordinator pursuant to 42 U.S.C. 300jj-11(c)(5) (ONC Health IT Certification Program).

© 2022 The Sequoia Project. All rights reserved.

Who Are the "Actors" Subject to Information Blocking Enforcement as Defined by ONC Regulation?

Health Information Network (HIN) or Health Information Exchange (HIE)	Health information network or health information exchange means 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 electronic health information: (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, as such terms are defined in 45 CFR 164.501 regardless of whether such individuals or entities are subject to the requirements of 45 CFR parts 160 and 164.

© 2022 The Sequoia Project. All rights reserved.

Information Blocking Revolves Around Practices

Information blocking **practices** include both affirmative acts and failures to act and may include:

- Restricting authorized access, exchange, or use of EHI,
- Implementing HIT in **nonstandard** ways*, and*
- Implementing HIT in ways that are likely to:
  - Restrict **access, exchange, or use** of **electronic health information (EHI)**, including for ***exporting complete information sets*** or ***transitioning between HIT systems***; or
  - Lead to fraud, waste, or abuse, or ***impede innovations and advancements*** in access, exchange, and use.

The ONC Final Rule identified "reasonable and necessary" activities (Exceptions) that are not information blocking (as called for by Cures). Both Proposed and Final Rules identified "practices" that could be information blocking and provided detailed examples.

113
© 2022 The Sequoia Project. All rights reserved.

The ONC Final Rule Defines a Broad Set of *Interoperability Elements* That Can Implicate Information Blocking

- Hardware, software, integrated technologies or related licenses, technical information, privileges, rights, intellectual property, upgrades, or services that:
  - (1) May be necessary to access, exchange, or use electronic health information; and
  - (2) Is/Are controlled by the Actor, which includes the ability to confer all rights and authorizations necessary to use the element to enable the access, exchange, or use of electronic health information.

© 2022 The Sequoia Project. All rights reserved.

Information Blocking: Penalties and Enforcement

- Health IT Developers, HINs/HIEs: Enforcement by ONC (developers) and/or HHS OIG—Penalties for not meeting certification conditions or false certification attestations (developers) and up to $1 million civil monetary penalties (CMPs) per violation (developers, HINs/HIEs)

- Health Care Providers: Enforcement and "disincentives" to be determined by forthcoming HHS rules, adding to existing CMS and OIG enforcement of CMS incentive program attestations re: "information blocking"

Applicability (Compliance)—As of 4/5/2021
Certification enforcement for Developers (ONC)—4/5/2021
Enforcement for HINs/HIEs and Developers by HHS OIG after forthcoming OIG Final Rule and forthcoming HHS proposed and final rules for Providers

© 2022 The Sequoia Project. All rights reserved.

Organizational Compliance Risks are Extensive

- Stiff fines and penalties
- Reputational risk
- Implementation and compliance costs
- Enforcement and regulatory uncertainty and conflicts (e.g., Cures vs. HIPAA)
- High EHI request volume
- Challenges in finding expertise and resources
- Many providers will seek to be patient information stewards, concerned about vetting apps and API access
- Enforcement may determine that what seemed compliant was not, with unexpected liability by an Actor

116
© 2022 The Sequoia Project. All rights reserved.

Addressing These Risks

Actors and potential Actors should:

- review applicable implementation and compliance issues,
- plan for the worst case,
- develop policies and procedures to ensure compliance, with some of these embedded in workflows,
- evaluate implications and obligations for parties with which you do business, including both threats and opportunities, and
- **adopt and adapt industry good practices, such as those in this report.**

117
© 2022 The Sequoia Project. All rights reserved.

Organizational Opportunities Will Also Be Created

- Organizational responses to information blocking and API regulatory requirements, and standards like the U.S. Core Data for Interoperability (USCDI) and HL7® FHIR®, will enable greater data access and integration of apps with existing health IT.
- Wider information sharing will provide opportunities for innovative healthcare organizations and health IT developers.
- Increased data access and integration will enable a broader "app economy," new technology approaches, data for artificial intelligence/machine learning, and broader and more useful provider/patient data use.

118
© 2022 The Sequoia Project. All rights reserved.

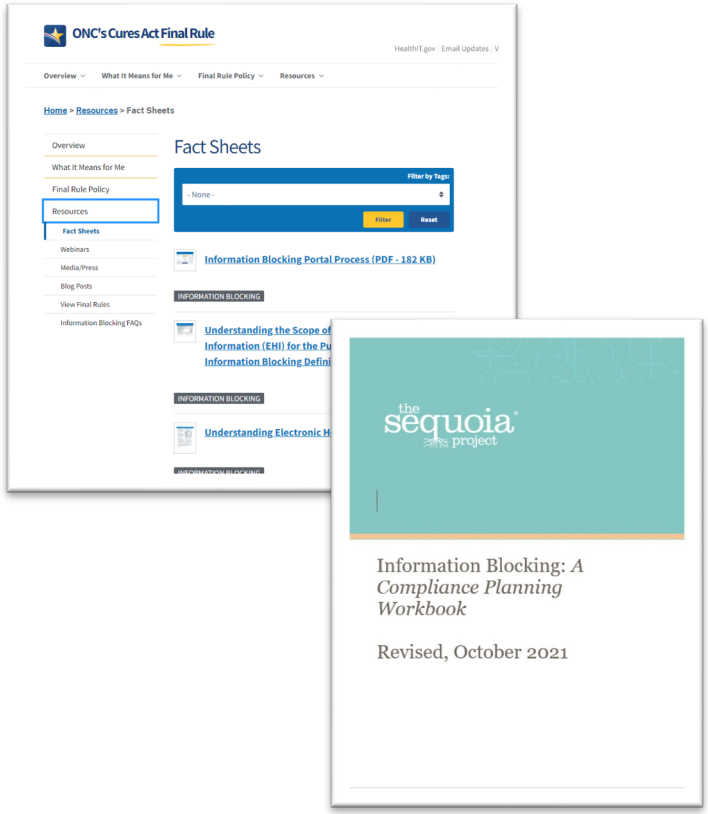
Careful Planning, Implementation and Compliance are Essential

- Organizations that are Actors or interact with Actors face many risks and opportunities from the information blocking regulations and ONC certified health IT open API requirements.
- They will need formal, organization-wide plans for compliance, operational and business responses to the Final Rule.
- Actors must avoid engaging in practices that result in information blocking or be sure that any such practices fit within one of the information blocking exceptions.
- Effective responses to the information blocking rules require engagement and support from the highest levels of an Actor organization and across the organization's teams.

© 2022 The Sequoia Project. All rights reserved.

Review ONC and other HHS Rules, FAQs and Stakeholder Educational Efforts for a Deeper Understanding

- ONC Resources: Rules, Fact Sheets, FAQs
- ONC Blog Posts
  - Pssst…Information blocking practices, your days are numbered…Pass it on. - Health IT Buzz
  - To share or not to share, what's an exception (to information blocking)? - Health IT Buzz
- Forthcoming HHS OIG Final Rule and forthcoming Provider enforcement regulations
- Sequoia and Stakeholder Resources



© 2022 The Sequoia Project. All rights reserved.