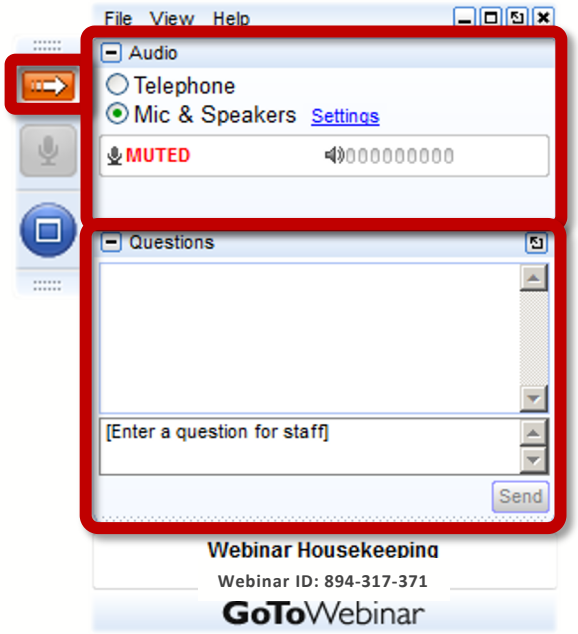
Information Blocking Compliance Bootcamp

Session 2: How Could an Organization Violate the Information Blocking Rule?

February 3, 2021

How To Participate Today



Your Participation

Open and close your control panel

Join audio:
- Choose "Mic & Speakers" to use VoIP
- Choose "Telephone" and dial using the information provided

Submit questions and comments via the Questions panel

Note: Today's presentation is being recorded and will be provided

Problems or Questions? Contact the Interoperability Matters Team at:

interopmatters@sequoiaproject.org

Bootcamp Goal and Objectives: Why Participate

Goal

The Bootcamp will provide carefully vetted, substantive resources and relevant information about requirements of the Information Blocking regulations and approaches to enhance effective and compliant organizational responses.

Objectives

1. Provide in-depth study of the Cures Act and the ONC and OIG Information Blocking rules, focusing on which organizations are Actors, prohibited practices, key definitions, regulatory exceptions, and penalties/"disincentives."
2. Deliver practical and useful guidance and tools to help participants design and implement regulatory compliance and implementation plans in their organizations.
3. Promote information sharing among participants during and after sessions.
4. Create a *Community of Interest* to encourage Bootcamp participants to continue sharing learnings and best practices after the Bootcamp concludes.

Meet The Sequoia Project Team

Mariann Yeager
CEO
The Sequoia Project

Steve Gravely
Founder & CEO
Gravely Group

Mark Segal
Principal
Digital Health Policy Advisors

About the Sequoia Project

The Sequoia Project is the independent, trusted advocate for nationwide health information exchange. In the public interest we steward current programs, incubate new initiatives, each with their own mission, governance, membership and structure, and educate our community.

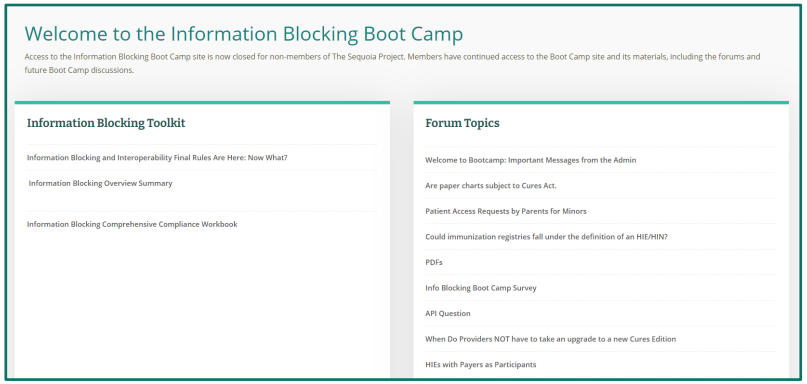
Information Blocking Compliance Boot Camp Sessions

✓ Information Blocking Overview	January 20, 2021
2. Violating the Information Blocking Rule	February 3, 2021
3. Exceptions: Part 1	February 17, 2021
4. Exceptions: Part 2	March 3, 2021
5. Enforcement Issues	March 17, 2021
6. Compliance: Part 1	March 31, 2021
7. Compliance: Part 2 and Wrap-Up	April 14, 2021

Bootcamp Materials

We have developed materials for you to use as part of the Bootcamp. These supplement, but do not replace, Bootcamp sessions.

- *Information Blocking Summary*—an extensive narrative that provides a comprehensive discussion of:
  - The legal authority for Information Blocking in the CURES Act, the ONC Final Rule, and the OIG Proposed Rule;
  - Key definitions and the exceptions.
- *Compliance Planning Workbook*—a comprehensive discussion of how to approach organizational compliance and implementation for Information Blocking with checklists, examples and suggestions.



https://sequoiaproject.org/2021-information-blocking-bootcamp/

Certificate of Participation

- Sequoia has invested extensive resources into this Bootcamp to provide participants with an excellent orientation to Information Blocking
- The core faculty, Steve Gravely and Mark Segal, are experts on the Information Blocking provisions
- The written materials have been carefully vetted for accuracy and objectivity
- Each session will include vital information and time for group discussion
- Participants are encouraged to share ideas and information outside of the bootcamp sessions
- All participants that attend each bootcamp session will receive a **Certificate of Completion** as tangible evidence of their achievement

Information Blocking Compliance Boot Camp: Office Hours

Between 3pm and 4pm ET on the following dates:

✓ January 27, 2021

2. February 10, 2021
3. February 24, 2021
4. March 10, 2021
5. March 24, 2021
6. April 7, 2021
7. April 21, 2021

Session 1 Recap

- ✓ Provide important administrative information to participants about the Bootcamp
- ✓ High-level discussion of Information Blocking for C-suite representatives from each Bootcamp participant
- ✓ In-depth discussion of the following topics:
  - What is Information Blocking?
  - Who is subject to the Information Blocking provisions?
  - What are the realistic risks and opportunities?

Sequoia's Goals

- Build an informed and engaged **Community of Practice**
- Reduce the organizational costs of "going it alone"
- Provide curated resources to the Community
- Facilitate two-way communications between regulators and the healthcare community
- Focus on ensuring that industry responses to the Information Blocking rules enhances and does not hinder continued growth in interoperability

Session Goals

- Explore how an organization could violate the Information Blocking rules
- Discuss the types of conduct that could get you into trouble and explore the idea of “practices”
- Include examples and discuss what ONC has said about practices, and why this provides a roadmap for your organization’s compliance planning
- Discuss the role that the intent of an Actor plays in violating the Information Blocking rules

Quick Refresher

Information Blocking is a **practice** that—

Except as **required by law** or covered by an **exception**, is likely to **interfere with-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**.

Practice is defined as an act or an omission

ONC's November 2020 Interim Final Rule with Comment corrected this definition to meet ONC intent and other relevant language—"does not constitute a substantive change"

Information Blocking Practices

Overview

Cures Identifies Information Blocking Practices: These Were Reflected in the ONC Final Rule

Information Blocking **practices** may include:

- Practices restricting authorized **access, exchange, or use** under applicable State or Federal law of **EHI** for **treatment and other permitted purposes** under such law, **including transitions between certified health IT**
- Implementing health IT **in nonstandard** ways likely to substantially increase the **complexity or burden** of access, exchange, or use; and
- Implementing health IT in ways likely to:
  - Restrict access, exchange, or use of EHI for **exporting complete information sets or transitioning between systems**; or
  - Lead to **fraud, waste, or abuse**, or **impede innovations** and **advancements** in access, exchange, and use, including health IT-enable care delivery

The Final Rule identified specific practices and examples and "reasonable and necessary" activities that are not Information Blocking (i.e., exceptions)

Practices: Changes in the Final Rule

- Did not revise list of 42 specific practice examples that could implicate Information Blocking listed in the Proposed Rule
- Added **new examples**
- Finalized purposes for access, exchange, or use for which interference will **almost always implicate Information Blocking**
  - e.g., patient access to EHI, treatment, care coordination
- Focuses on actors with **control** over interoperability elements

The Critical Role of Intent and Knowledge

Cures "defines information blocking broadly and . . . allows for careful consideration of relevant facts and circumstances in individual cases, which includes analysis of an *actor's intent* and whether it meets the *requisite knowledge* standard" (Final Rule, p. 25820)

- **Intent:** For example, ONC states that "[f]ees that do not meet this [Fees] exception may implicate the information blocking provision and will have to be assessed on a case-by-case basis to determine, for example, the actor's intent and whether the practice rises to the level of an interference." (p. 25880)
    - **Unlike the Stark law, Information Blocking does not use "strict liability"**
- **Knowledge**: Developers and HINs/HIEs are held to a "knows or should know" standard. Providers are held to a "knows" standard

Discussion

Examples of Practices

Restrictions on Access, Exchange, or Use

- Requiring consent to exchange EHI for treatment **even though not required by law**
- Developer **refuses to share technical information needed** to **export data**
- HIN restriction on end-user sharing EHI with **non-HIN members**
- Vendor **only provides EHI in PDF** on termination of customer agreement
- Developer of certified health IT **refuses to license interoperability elements reasonably necessary** for others to develop and deploy software that works with health IT

Restrictions on Access, Exchange, or Use

- An actor may want to engage an entity for services (e.g., use of a CDS application that require the CDS App Developer to enter into a BAA with a provider and to gain access to and use EHI held by another BA of the provider [e.g., EHR developer of certified health IT]), and the **CDS Developer is required by the EHR developer to enter into a contract to access its EHR**
  - **"[C]ontracts and agreements can interfere with the access, exchange, and use of EHI through terms besides those that specify unreasonable fees and commercially unreasonable licensing terms"**

Limiting or Restricting the Interoperability of Health IT

- Actor deploys technological measures that **restrict ability to reverse engineer** to develop means for extracting and using EHI in the technology
- Hospital directs EHR developer to configure technology **so users cannot easily send electronic referrals to unaffiliated providers**, even when the user knows Direct address and/or identity of the unaffiliated provider
- Developer prevents (e.g., by **exorbitant fees** unrelated to costs or by technology) third-party CDS app from **writing EHI to EHR as requested by provider**
- Provider **has capability to provide same-day access** to EHI but takes several days to respond

Limiting or Restricting the Interoperability of Health IT

- A **FHIR service base URL** (i.e., "FHIR endpoints") cannot be withheld by an actor as it (just like many other technical interfaces) is **necessary to enable the access, exchange, and use of EHI**
- **Slowing or delaying access, exchange, or use of EHI could constitute an "interference"** and implicate Information Blocking; for example, **scoping and architecture questions** could constitute interference and implicate Information Blocking if not necessary to enable access, exchange, or use of EHI and **utilized as a delay tactic**

Impeding Innovations and Advancements in Access, Exchange, or Use or Health IT-Enabled Care Delivery

- Developer of certified health IT requires third-party apps to be "vetted" for security but **does not vet promptly**
- Developer of certified health IT **refuses to license interoperability elements that other applications require** to access, exchange, and use EHI in the developer's technology
- Provider engages integrator to develop interface engine but its **license with EHR developer prohibits it from disclosing technical documentation integrator needs** to perform the work [**without broad non-compete**]
- **Health system insists local physicians adopt its EHR platform**, which provides **limited connectivity with competing hospitals** and threatens to revoke admitting privileges for physicians that do not comply
- HIN charges additional fees, requires more stringent testing or certification requirements, or **imposes additional terms for participants that are competitors**, are potential competitors, or may use EHI obtained via the HIN in a way that facilitates competition with the HIN

Impeding Innovations and Advancements in Access, Exchange, or Use or Health IT-Enabled Care Delivery

- **App vetting and "education"**
  - Practices that educate patients about app privacy and security of parties to whom a patient chooses to receive EHI may be reviewed by OIG or ONC if Information Blocking is claimed
  - ONC states that these practices are unlikely to interfere with access, exchange, and use if information:
    - **Focuses on current privacy and/or security risks** posed by the technology or the third-party developer of the technology
    - Is **factually accurate, unbiased, objective**, and not unfair or deceptive
    - Provided in a **non-discriminatory** manner
  - **An actor may not prevent an individual from deciding to provide EHI to a technology developer or app despite risks noted regarding the app or developer**
  - Actors may establish processes to notify a patient, call to a patient's attention, or display in advance whether developer of app patient is about to authorize to receive EHI has attested that its privacy policy and security practices meet "best practices"
  - ONC provides minimum app privacy notice criteria and examples

App Vetting and "Education": ONC FAQ

Q: Will educating patients about the privacy and security risks posed by third-party apps that the patient chooses be considered interference? +

It will not be considered an "interference" with the access, exchange, or use of EHI if:

- Foremost, the information provided by actors must focus on any current privacy and/or security risks posed by the technology or the third-party developer of the technology;
- Second, this information must be factually accurate, unbiased, objective, and not unfair or deceptive; and
- Finally, the information must be provided in a non-discriminatory manner.

For example, actors may establish processes where they notify a patient, call to a patient's attention, or display in advance (as part of the app authorization process within certified API technology) whether the third-party developer of the app that the patient is about to authorize to receive their EHI has attested in the positive or negative as to whether the third party's privacy policy and practices (including security practices) meet particular benchmarks. However, such processes must be non-discriminatory in that they must be used in the same manner for all third-party apps/developers.

App **V**etting and "Education": ONC FAQ (2)

The particular benchmarks an actor might identify in this example could be the minimum expectations described below, more stringent "best practice" expectations that may be set by the market, or some combination of minimum and "best practice" expectations. As described in the Final Rule at 85 FR 25816, all third-party privacy policies and practices should, at a minimum, adhere to the following:

- The privacy policy is made publicly accessible at all times, including updated versions;
- The privacy policy is shared with all individuals that use the technology prior to the technology's receipt of EHI from an actor;
- The privacy policy is written in plain language and in a manner calculated to inform the individual who uses the technology;
- The privacy policy includes a statement of whether and how the individual's EHI may be accessed, exchanged, or used by any other person or other entity, including whether the individual's EHI may be sold at any time (including in the future); and
- The privacy policy includes a requirement for express consent from the individual before the individual's EHI is accessed, exchanged, or used, including receiving the individual's express consent before the individual's EHI is sold (other than disclosures required by law or disclosures necessary in connection with the sale of the application or a similar transaction).

Rent-Seeking and Other Opportunistic Pricing Practices

- Developer of certified health IT **charges customers a fee exceeding their costs** for interfaces, connections, data export, data conversion or migration, other interoperability services
- Developer of certified health IT **charges more to export or use EHI in certain competitive situations** or purposes
- **Developer of certified health IT interposes itself between customer and third-party developer**, insisting that developer pay licensing fee, royalty, or other payment [not related to costs] for permission to access EHR or documentation
- Analytics company provides services to customers of developer of certified health IT and **developer insists on revenue sharing that exceeds its reasonable costs**

Practices: Information Blocking Workgroup Comments

- The definition of **interoperability elements** is broad (beyond certified health IT) and interacts with **practices** and **actors** (and other parts of the rule) to create wide and complex compliance risk
- Although used in Cures, the **term "likely" in the regulatory definition of Information Blocking is problematic** without a commonly understood definition
- **Regulators need to allow due diligence as distinct from simply delaying access**; such diligence **should not need an exception** (e.g., the Security exception) to avoid being viewed as Information Blocking

Practices: Information Blocking Workgroup Comments

- The **focus on non-standard implementations, along with the broad definitions of actors, could pose challenges for some organizations** (e.g., registries) that often need non-standard implementations
- ONC should provide **more examples of non-standard implementation** for when adopted standards exist and when they do not
- The **rule seems to assume actors have bad intent**, and to err on the side of ensuring that there are no loopholes for these bad actors to exploit. This approach casts a wide net and there is a strong chance of collateral damage and pulling in those acting in good faith

Business Associate Agreements: ONC Final Rule (1)

- "We designed the final rule to operate in a manner consistent with the framework of the HIPAA Privacy Rule and other laws providing privacy rights for patients. Foremost, we do not require the disclosure of EHI in any way that would not already be permitted under the HIPAA Privacy Rule (or other federal or state law). **However, if an actor is *permitted* to provide access, exchange, or use of EHI under the HIPAA Privacy Rule (or any other law), then the Information Blocking provision would require that the actor provide that access, exchange, or use of EHI so long as the actor is not prohibited by law from doing so (assuming that no exception is available to the actor)."**
- According to ONC, while the Information Blocking provision does not require Actors to violate a BAA, a **BAA or its associated service level agreements must not be used in a discriminatory manner by an actor to forbid or limit disclosures that otherwise would be permitted** by the Privacy Rule.
  - For example, a **BAA entered into by one or more Actors that permits access, exchange, or use of EHI by certain health care providers for treatment should generally not prohibit or limit the access, exchange, or use of the EHI for treatment by other health care providers** of a patient.

Business Associate Agreements: ONC Final Rule (2)

- **According to ONC, both the provider(s) who initiated the BAA and the Business Associate (BA) who may be an Actor under the Information Blocking provision (e.g., a developer of certified health IT) could be subject to Information Blocking enforcement.**
  - To illustrate the potential culpability of a BA, **a BA with significant market power may have contractually prohibited or made it difficult for its covered entity customers to exchange EHI**, maintained by the BA, with health care providers that use an EHR system of one of the BA's competitors.
  - To determine whether there is Information Blocking, the **actions and processes (e.g., negotiations) of the Actors in reaching the BAA and associated service level agreements would need to be reviewed to determine whether there was any action taken by an Actor that was likely to interfere with the access, exchange, or use of EHI, and whether the Actor had the requisite intent**.
  - If the BA has an agreement with the covered entity to provide EHI to a third party that requests it and the BA refuses to provide the access, exchange, or use of EHI to a requestor in response to the request received by the CE, the **BA (who is also an Actor under the Information Blocking provision) may have violated the Information Blocking provision unless an exception applied.**

Business Associate Agreements: ONC FAQ

Q: Does the information blocking regulation require actors to violate existing business associate agreements in order to not be considered an information blocker?

No. The information blocking regulation in 45 CFR part 171 do not require actors to violate business associate agreements (BAA) or associated service level agreements. However, the terms or provisions of such agreements could constitute an interference (and thus could be information blocking) if used in a discriminatory manner by an actor to limit or prohibit the access, exchange, or use of electronic health information (EHI) for treatment purposes that otherwise would be permitted by the Privacy Rule. For example, a BAA entered into by one or more actors that permits access, exchange, or use of EHI by certain health care providers for treatment should generally not prohibit or limit the access, exchange, or use of the EHI for treatment by other health care providers of a patient. See also the section discussing business associate agreements in the Final Rule at 85 FR 25812.

Discussion

Coming Up In The Next Session

Session 3: Exceptions Part 1

- This initial session on the topic of Exceptions will be an overview of the way ONC organizes the exceptions in the Final Rule, and what we can infer from the changes made between the proposed and final rule
- We will review the elements of the exceptions and what it means to meet an exception and to document compliance
- We will also begin detailed review of the Preventing Harm, Privacy, Security, and Health IT Performance Exceptions

Interoperability Matters

https://sequoiaproject.org/interoperability-matters/