Information Blocking Workgroup Meeting #2

Interoperability Matters

3/25/2019

the sequoia project

Agenda

- Welcome and Introductions
- Workgroup Overview Refresh
- Actors and Other Definitions
  - Providers
  - CEHRT Developers
  - HIEs
  - HINs
- Information Blocking Practices
- Exceptions
  - Harm
  - Privacy
  - Security
- Next Steps

The Sequoia Project Team

Lindsay Austin, Troutman Sanders Strategies

Didi Davis, VP, Informatics, Conformance & Interoperability

Steve Gravely, Gravely Group - Facilitator

Shawna Hembree, Program Manager

Mark Segal, Digital Health Policy Advisors - Facilitator

Dawn VanDyke, Director, Marketing Communications

Mariann Yeager, CEO

Purpose

- Identify practical, implementation-level implications of proposed and final information blocking rules, which may or may not be consensus positions
- Provide input into Sequoia comments to ONC on proposed rule
- Facilitate ongoing discussions to clarify information blocking policies and considerations prior to and after the Final Rule

Workgroup Representatives

Associations and Orgs - health IT community
- Tom Leary / Mari Greenberger, HIMSS*
- Matt Reid, AMA
- Lauren Riplinger, AHIMA
- Scott Stuewe, DirectTrust

Consumers
- Ryan Howells, CARIN Alliance
- Deven McGraw, Ciitizen

Federal Government
- Steve Bounds, SSA*
- Margaret Donahue, VA

Health Information Networks and Service Providers
- Angie Bass, Missouri Health Connect
- Dave Cassel, Carequality
- Laura Danielson, Indiana Health Information Exchange
- Paul Uhrig, Surescripts, Co-Chair

Healthcare Provider
- David Camitta, Dignity, Co-Chair
- Eric Liederman, Kaiser Permanente

**Invited*

Legal, Technology, Standards, and Policy Subject Matter Experts
- Jodi Daniel, Crowell & Moring, LLP
- Josh Mandel, Microsoft
- Micky Tripathi, MaEHC

Payers
- Nancy Beavin, Humana
- Danielle Lloyd, AHIP
- Matthew Schuller, BCBSA*

Public Health
- John Loonsk, Johns Hopkins University

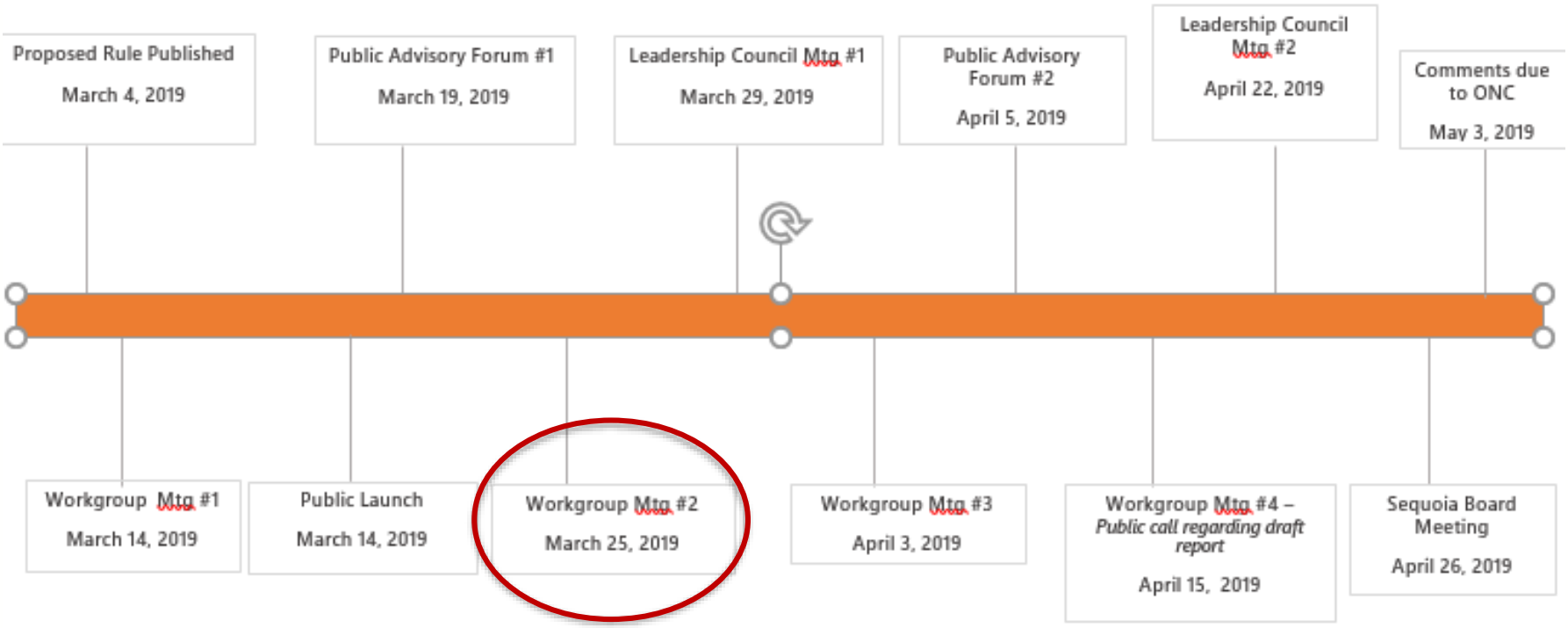
Vendors
- Brian Ahier, Medicity / Health Catalyst
- Aashima Gupta, Google
- Cherie Holmes-Henry, EHRA / NEXTGEN
- Rob Klootwyk, Epic
- Josh Mast, Cerner

Informatics
- Doug Fridsma, AMIA

Safety net providers / service provider
- Jennifer Stoll, OCHIN

Release of Information Company
- Rita Bowen, MROCorp

Key Milestones



Confirmed Times and Registration for Public Calls will be posted at https://sequoiaproject.org/events/

Criteria for Workgroup Review

- *ONC basis* for selecting exceptions:
  - Each is limited to certain activities that *clearly advance the aims* of the information blocking provision
  - Each addresses a *significant risk that regulated actors will not engage in these beneficial activities* because of uncertainty concerning the breadth or applicability of the information blocking provision
  - Each is *subject to strict conditions* to ensure that it is limited to activities that are reasonable and necessary
- *Impact* of a practice and exception
- *Likely benefit* per Congressional intent and by actor/party
- *Implementation*: feasibility & complexity, cost & burden: by actor/party
- *Compliance: challenges*, uncertainties, potential best practices
- *Unintended consequences*

Rules of the Road

- We want to hear from you!
- Let's focus on highest priority points and themes
- We encourage use of chat during the meeting to make points and we will capture the chat logs
- Send us your thoughts between meetings
  - interopmatters@sequoiaproject.org
  - Reference "Workgroup" in message header

Actors Defined §171.102 – Focus of WG #2

Health Care Providers	Same meaning as "health care provider" at 42 U.S.C. 300jj—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.
Health IT Developers of Certified Health IT	An individual or entity that develops or offers health information technology (as that term is defined in 42 U.S.C. 300jj(5)) and which had, at the time it engaged in a practice that is the subject of an information blocking claim, health information technology (one or more) certified under the ONC Health IT Certification Program
Health Information Exchanges	Individual or entity that enables access, exchange, or use of electronic health information primarily between or among a particular class of individuals or entities or for a limited set of purposes
Health Information Networks	Health Information Network or HIN means an individual or entity that satisfies one or both of the following— (1) Determines, oversees, administers, controls, or substantially influences policies or agreements that define business, operational, technical, or other conditions or requirements for enabling or facilitating access, exchange, or use of electronic health information between or among two or more unaffiliated individuals or entities (2) Provides, manages, controls, or substantially influences any technology or service that enables or facilitates the access, exchange, or use of electronic health information between or among two or more unaffiliated individuals or entities

HIEs and HINs

HIE

- Include but not limited to RHIOs, state HIEs, other organizations, entities, or arrangements that enable EHI to be accessed, exchanged, or used between or among particular types of parties or for particular purposes
- Might facilitate or enable access, exchange, or use exclusively within a region, or for a limited scope of participants and purposes (e.g., registry or exchange established by hospital-physician organization to facilitate ADT alerting)
- May be established for specific health care or business purposes or use cases
- If facilitates access, exchange, or use for more than a narrowly defined set of purposes, may be HIE and a HIN

HIN

- Entity established in a state to improve movement of EHI between providers operating in state; identifies standards for security and offers Ts and Cs for providers wishing to participate in the network.
- Entity offering (and overseeing and administering) Ts and Cs for network participation
- Health system administers agreements to facilitate exchange of EHI for use by unaffiliated family practices and specialist clinicians to streamline referrals
- Individual or entity that does not directly enable, facilitate, or control movement of information, but exercises control or substantial influence over policies, technology, or services of a network
- A large provider may decide to lead effort to establish a network that facilitates movement of EHI between group of smaller providers (and the large provider) and through technology of health IT developers; large provider, with some participants, creates a new entity that administers network's policies and technology
- Note: Network is never defined

Are distinctions clear? Too broad or too narrow? Consistent with congressional intent?

Actors: Recommendations

Information Blocking Practices

Cures Statute

- (A) practices that restrict authorized *access*, *exchange*, or *use* under applicable State or Federal law of such information for *treatment and other permitted purposes* under such applicable law, including transitions between certified health information technologies;
- (B) implementing health information technology in *nonstandard* ways that are likely to substantially increase the complexity or burden of accessing, exchanging, or using electronic health information;
- (C) implementing health information technology in ways that are likely to— ‘‘(i) restrict the access, exchange, or use of electronic health information with respect to *exporting complete information sets* or in *transitioning between health information technology systems*;
- or ‘‘(ii) lead to fraud, waste, or abuse, or *impede innovations and advancements* in health information access, exchange, and use, including care delivery enabled by health information technology.

Proposed Rule

- Restrictions on access, exchange, or use of EHI *through formal means (e.g., contractual restrictions) or informal means (e.g., ignoring requests to share EHI)*
- *Limiting or restricting the interoperability of health IT* (e.g., disabling a capability that allows users to share EHI with users of other systems)
- Impeding innovations and advancements in access, exchange, or use or health IT-enabled care delivery *(e.g., refusing to license interoperability elements to others who require such elements to develop and provide interoperable services)*
- *Rent-seeking and other opportunistic pricing practices* (e.g., charging fees to provide interoperability services that exceed actual costs incurred to provide the services)
- Non-standard implementation practices *(e.g., choosing not to adopt relevant standards, implementation specifications, and certification criteria)*

ONC examples in Background. Too broad or too narrow? Consistent with congressional intent?

Practice: Recommendations

Information Blocking: "Reasonable and Necessary" Exceptions

- If *practice* satisfies one or more exceptions, *actor* would not be treated as *information blocking* and not subject to penalties and disincentives
  - Most exceptions apply to all actors, unless otherwise indicated
- Consistent themes across exceptions (e.g., pro-competitive, consistent, non-discriminatory, policies in place and documented compliance with these policies)
- *Must generally meet all elements at all relevant times to satisfy an exception for each practice where an exception is claimed*
  - Rather than "substantial compliance" (e.g., HIPAA)
- The actor has the burden of proving compliance with the exception in the event of an investigation

ONC Policy Considerations for Exceptions

1. Each is limited to certain *activities that clearly advance the aims of the information blocking provision*
2. Each addresses a significant *risk that regulated actors will not engage in these beneficial activities because of uncertainty* concerning the breadth or applicability of the information blocking provision
3. Each is subject to *strict conditions to ensure that it is limited to activities that are reasonable and necessary*

Exception: Preventing Harm

- An actor may engage in practices that are reasonable and necessary to prevent *harm* to a patient or another person
- The actor must have a reasonable belief that the practice will directly and substantially reduce the likelihood of harm (special focus on physical harm) to a patient or another person
- The practice must implement an *organizational policy* that meets certain requirements *or* must be based on an *individualized assessment of the risk in each case*

42 CFR Part 2 and ability to isolate records that could lead to harm (e.g., in notes).
Is the focus on physical harm appropriate?

Exception: Preventing Harm

To qualify for this exception, each practice by an actor must meet the following conditions at *all* relevant times.

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

(1) Corrupt or inaccurate data being recorded or incorporated in a patient's electronic health record;

(2) Misidentification of a patient or patient's electronic health information; **or**

(3) Disclosure of a patient's electronic health information in circumstances where a licensed health care professional has determined, in the exercise of professional judgment, that the disclosure is reasonably likely to endanger the life or physical safety of the patient or another person, provided that, if required by applicable federal or state law, the patient has been afforded any right of review of that determination.

(b) If the practice implements an organizational policy, the policy must be—

(1) In writing;

(2) Based on relevant clinical, technical, and other appropriate expertise;

(3) Implemented in a consistent and non-discriminatory manner; **and**

(4) No broader than necessary to mitigate the risk of harm.

(c) If the practice does not implement an organizational policy, an actor must make a finding in each case, based on the particularized facts and circumstances, and based on, as applicable, relevant clinical, technical, and other appropriate expertise, that the practice is necessary and no broader than necessary to mitigate the risk of harm.

Preventing Harm: Recommendations

Exception: Promoting the Privacy of Electronic Health Information

- An actor may engage in practices that protect the privacy of EHI
- An actor must satisfy *at least one of four* discrete sub-exceptions that address scenarios that recognize existing privacy laws and privacy-protective practices:
  1. Practices that satisfy preconditions prescribed by privacy laws;
  2. Certain practices not regulated by HIPAA but that implement documented and transparent privacy policies;
  3. Denial of access practices that are specifically permitted under HIPAA; or
  4. Practices that give effect to an individual's privacy preferences.
- Actors need not provide access, exchange, or use of EHI in a manner not permitted under the HIPAA Privacy Rule
- General conditions apply to ensure that practices are tailored to the specific privacy risk or interest being addressed and implemented in a *consistent and non-discriminatory manner*

Are non-HIPAA entities sufficiently addressed?
Organizational policies (some could be information blocking practice; others could enable exception)

Exception: Promoting the Privacy of Electronic Health Information

To qualify for this exception, each practice by an actor must satisfy at least one of the sub-exceptions in paragraphs (b) through (e) of this section at all relevant times.

(a) *Meaning of "individual" in this section*. The term "individual" as used in this section means one or more of the following—

(1) An individual as defined by 45 CFR 160.103.

(2) Any other natural person who is the subject of the electronic health information being accessed, exchanged, or used.

(3) A person who legally acts on behalf of a person described in paragraph (a)(1) or (2) of this section, including as a personal representative, in accordance with 45 CFR 164.502(g).

(4) A person who is a legal representative of and can make health care decisions on behalf of any person described in paragraph (a)(1) or (2) of this section.

(5) An executor, administrator or other person having authority to act on behalf of a deceased person described in paragraph (a)(1) or (2) of this section or the individual's estate under State or other law.

(b) *Precondition not satisfied.* If the actor is required by a state or federal privacy law to satisfy a condition prior to providing access, exchange, or use of electronic health information, the actor may choose not to provide access, exchange, or use of such electronic health information if the precondition has not been satisfied, provided that—

(1) The actor's practice—

(i) Conforms to the actor's organizational policies and procedures that:

(A) Are in writing;

(B) Specify the criteria to be used by the actor and, as applicable, the steps that the actor will take, in order that the precondition can be satisfied; **and**

(C) Have been implemented, including by taking reasonable steps to ensure that its workforce members and its agents understand and consistently apply the policies and procedures; **or**

(ii) Has been documented by the actor, on a case-by-case basis, identifying the criteria used by the actor to determine when the precondition would be satisfied, any criteria that were not met, and the reason why the criteria were not met; and

Exception: Promoting the Privacy of Electronic Health Information

(2) If the precondition relies on the provision of consent or authorization from an individual, the actor:

(i) Did all things reasonably necessary within its control to provide the individual with a meaningful opportunity to provide the consent or authorization; and

(ii) Did not improperly encourage or induce the individual to not provide the consent or authorization.

(3) The actor's practice is—

(i) Tailored to the specific privacy risk or interest being addressed; and

(ii) Implemented in a consistent and non-discriminatory manner.

(c) Health IT developer of certified health IT not covered by HIPAA. If the actor is a health IT developer of certified health IT that is not required to comply with the HIPAA Privacy Rule when engaging in a practice that promotes the privacy interests of an individual, the actor may choose not to provide access, exchange, or use of electronic health information provided that the actor's practice—

(1) Complies with applicable state or federal privacy laws;

(2) Implements a process that is described in the actor's organizational privacy policy;

(3) Had previously been meaningfully disclosed to the persons and entities that use the actor's product or service;

(4) Is tailored to the specific privacy risk or interest being addressed; and

(5) Is implemented in a consistent and non-discriminatory manner.

(d) Denial of an individual's request for their electronic protected health information in the circumstances provided in 45 CFR 164.524(a)(1), (2), and (3). If an individual requests their electronic protected health information under 45 CFR 164.502(a)(1)(i) or 45 CFR 164.524, the actor may deny the request in the circumstances provided in 45 CFR 164.524(a)(1), (2), or (3).

(e) Respecting an individual's request not to share information. In circumstances where not required or prohibited by law, an actor may choose not to provide access, exchange, or use of an individual's electronic health information if—

(1) The individual requests that the actor not provide such access, exchange, or use;

(2) Such request is initiated by the individual without any improper encouragement or inducement by the actor;

(3) The actor or its agent documents the request within a reasonable time period; and

(4) The actor's practice is implemented in a consistent and non-discriminatory manner.

Protecting Privacy: Recommendations

Exception: Promoting the Security of Electronic Health Information

- An actor may implement measures to promote the security of EHI
  - The practice must be directly related to safeguarding the confidentiality, integrity, and availability of EHI
  - The practice must be tailored to specific security risks and must be implemented in a consistent and non-discriminatory manner
  - The practice must implement an organizational security policy that meets certain requirements or must be based on an individualized determination regarding the risk and response in each case

Are non-HIPAA entities sufficiently addressed?
Organizational policies (some could be information blocking practice; others could enable exception)

Exception: Promoting the Security of Electronic Health Information

To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.

(a) The practice must be directly related to safeguarding the confidentiality, integrity, and availability of electronic health information.

(b) The practice must be tailored to the specific security risk being addressed.

(c) The practice must be implemented in a consistent and non-discriminatory manner.

(d) If the practice implements an organizational security policy, the policy must—

(1) Be in writing;

(2) Have been prepared on the basis of, and directly respond to, security risks identified and assessed by or on behalf of the actor;

(3) Align with one or more applicable consensus-based standards or best practice guidance; **and**

(4) Provide objective timeframes and other parameters for identifying, responding to, and addressing security incidents.

(e) If the practice does not implement an organizational security policy, the actor must have made a determination in each case, based on the particularized facts and circumstances, that:

(1) The practice is necessary to mitigate the security risk to the electronic health information; **and**

(2) There are no reasonable and appropriate alternatives to the practice that address the security risk that are less likely to interfere with, prevent, or materially discourage access, exchange or use of electronic health information.

Protecting Security: Recommendations

Final Thoughts and Next Steps

- Next meeting is April 3
- Final meeting before comments are due is April 15 with public invited to listen and comment at end
- Please send any follow-up thoughts on topics addressed by March 29

Interoperability Matters

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