Information Blocking:
A Policy Perspective

Mark J. Segal, PhD, FHIMSS
Principal, Digital Health Policy Advisors, LLC
Chair, HL7 Policy Advisory Committee
msegal@dig-hpa.com

HIMSS18
March 7, 2018
21st Century Cures and Information Blocking

- Landmark US federal healthcare innovation law
- HIT: interoperability, “information blocking,” transparency, safety
- Creates obligations re: information blocking for developers, health information networks, and providers
- Links to ONC certification but obligations and risks extend beyond certified products to overall company actions
- HHS to issue certification regulation within one year of enactment - 12/2017 & regulation on “reasonable and necessary” with no due date: Expected April 2018
- Enforcement mostly by HHS OIG—fines up to $1M per violation
- Requires compliance and risk management strategy - product, services, commercial, support, legal, regulatory
SEC. 4004. INFORMATION BLOCKING

SEC. 3022. INFORMATION BLOCKING.

‘Information Blocking’ means a practice that—

(A) except as required by law or specified by the Secretary pursuant to rulemaking under paragraph (3), is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information; and

(B) (i) if conducted by a HIT developer, exchange, or 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

(ii) 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.

Very broad definition, not limited in B(i) to developers of certified HIT (only they attest), “know or should know,” “likely,” “knows . . unreasonable” only part of provider definition
Further detail on specific practices that restrict legally permitted access, exchange or use, including customers changing certified HIT; nonstandard implementation (beyond not using standards) that increase complexity or burden for customer or authorized data user (e.g., unique database structure?)
SEC. 4004. INFORMATION BLOCKING

SEC. 3022. INFORMATION BLOCKING (Continued)

(C) implementing HIT 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 HIT 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 HIT.

Focus on exporting “complete information sets” (e.g., beyond CCDA to registries, patients, etc.) and in changing from one HIT system to another (not just certified); focus on “innovations and advancements” (e.g., apps and APIs).
This rule will be critically important and should draw on prior ONC report on information blocking as a starting point re: “reasonable”. Required rulemaking has no deadline (but see next section on enforcement). Issue of “necessary” also needs careful consideration, focused on what is needed for viable businesses.
“Such technology,” used elsewhere also, seems to relate to certified HIT. It will be essential to confirm such an understanding as it drives vendor obligations.
SEC. 4004. INFORMATION BLOCKING

SEC. 3022. INFORMATION BLOCKING (Continued)
(b) INSPECTOR GENERAL AUTHORITY.—
(1) IN GENERAL.—The HHS inspector general may investigate any claim that—
(A) a HIT developer of certified health information technology or other entity offering certified HIT—
(i) submitted a false attestation under 3001(c)(5)(D)(vii); or (ii) engaged in information blocking;
(B) a health care provider engaged in information blocking; or
(C) a health information exchange or network engaged in information blocking.

For developers, limited to those who develop or offer certified HIT. Focus on false attestation and information blocking). OIG has stated no enforcement prior to “reasonable and necessary” rulemaking.
Note size of potential penalty per violation. OIG determination implied to be fact specific considering specified factors, including extent and actual harm. No limit of obligation to certified HIT.
SEC. 4004. INFORMATION BLOCKING

SEC. 3022. INFORMATION BLOCKING (Continued)

(B) PROVIDERS.—Any individual or entity described in subparagraph (B) of paragraph (1) determined by the Inspector General to have committed information blocking shall be referred to the appropriate agency to be subject to appropriate disincentives using authorities under applicable Federal law, as the Secretary sets forth through notice and comment rulemaking.

(C) PROCEDURE.—The provisions of section 1128A of the Social Security Act (other than subsections (a) and (b) of such section) shall apply to a civil money penalty applied under this paragraph in the same manner as such provisions apply to a civil money penalty or proceeding under such section 1128A(a).

(D) RECOVERED PENALTY FUNDS.—The amounts recovered under this paragraph shall be allocated to cover cost of enforcement with the remainder to the Medicare trust funds.

(E) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to the OIG to carry out this section $10,000,000

Note less specific penalties for providers, TBD via HHS rulemaking. See also size of OIG enforcement rule-making appropriation ($10 million).
SEC. 4004. INFORMATION BLOCKING

SEC. 3022. INFORMATION BLOCKING (Continued)

(3) RESOLUTION OF CLAIMS.—

(A) IN GENERAL.—The OIG, if such Office determines that a consultation regarding the HIPAA health privacy and security rules will resolve an information blocking claim, may refer such instances of information block to the HHS OCR resolution.

(B) LIMITATION ON LIABILITY.—If a provider or HIT developer makes information available based on a good faith reliance on consultations with the OCR pursuant to a referral under subparagraph (A), with respect to such information, the health care provider or developer shall not be liable for such disclosure or disclosures made pursuant to subparagraph (A).

Crossover of HIPAA privacy/security basis for information blocking concerns and some protection for vendor and provider provision of information for this limited reason.
SEC. 4004. INFORMATION BLOCKING

SEC. 3022. INFORMATION BLOCKING (Continued)

(c) IDENTIFYING BARRIERS TO EXCHANGE OF CERTIFIED HEALTH INFORMATION TECHNOLOGY.—

(1) (TRUSTED EXCHANGE DEFINED.—In this section, the term ‘trusted exchange’ with respect to certified electronic health records (CEHRT) means that the certified electronic health record technology has the technical capability to enable secure health information exchange between users and multiple certified electronic health record technology systems.

(2) GUIDANCE.—The National Coordinator, in consultation with the OCR, shall issue guidance on common legal, governance, and security barriers that prevent the trusted exchange of electronic health information.

(3) REFERRAL.—The National Coordinator and the OCR may refer to the OIG instances or patterns of refusal to exchange health information using CEHRT that is technically capable of trusted exchange and under conditions when exchange is legally permissible.

Focus on technical capabilities of CEHRT—key provision looks to ONC and OCR referrals to OIG based on refusal to use CEHRT capabilities for exchange.
SEC. 4004. INFORMATION BLOCKING

SEC. 3022. INFORMATION BLOCKING (Continued)

(3) STANDARDIZED PROCESS.—

(A) IN GENERAL.—The National Coordinator shall implement a standardized process for the public to submit reports on claims of—

(i) HIT products or developers of such products (or other entities offering such products to health care providers) not being interoperable or resulting in information blocking;

(ii) actions described in subsection (b)(1) that result in information blocking as described in subsection (a); and

(iii) any other act described in subsection (a).

(B) COLLECTION OF INFORMATION.—The standardized process implemented under subparagraph (A) shall provide for the collection of such information as the originating institution, location, type of transaction, system and version, timestamp, terminating institution, locations, system and version, failure notice, and other related information.

(4) NONDUPLICATION OF PENALTY STRUCTURES.—In carrying out this subsection, the Secretary shall, to the extent possible, ensure that penalties do not duplicate penalty structures that would otherwise apply with respect to information blocking and the type of individual or entity involved as of the day before the date of the enactment of this section.”
SEC. 4002. TRANSPARENT REPORTING ON USABILITY, SECURITY, AND FUNCTIONALITY: Enhancements to Certification

(D) CONDITIONS OF CERTIFICATION.—

Not later than 1 year after enactment, the HHS Secretary, through notice and comment rule making, shall require, as a condition of certification and maintenance of certification that the HIT developer:

(i) does not take any action that is information blocking as defined in section 3022(a)

(ii) provides assurances that it, unless for legitimate purposes specified by the Secretary, will not take any action described in clause (i) (information blocking) or any other action that may inhibit the appropriate exchange, access, and use of electronic health information;

Key concepts: New certification requirement, 1 year timeline for rule-making, link to statutory information blocking definition, assurances create liabilities, reference to HHS-specified “legitimate purposes,” “any other action . .”. Note: actions are focused on the developer (e.g., company), not just certified HIT.
SEC. 4002. TRANSPARENT REPORTING ON USABILITY, SECURITY, AND FUNCTIONALITY: Enhancements to Certification

(D) CONDITIONS OF CERTIFICATION.— (Continued)

(iii) does not prohibit or restrict communication regarding

(I) the usability, (II) the interoperability HIT, or (III) the security of the HIT

(IV) relevant information regarding users’ experiences when using the HIT

(V) the business practices of HIT developers related to exchanging electronic health information; and

(VI) the manner in which a user of the HIT has used such technology

(iv) has published APIs and allows health information from such technology to be accessed, exchanged, and used without special effort through the use of APIs or successor technology or standards, as provided for under applicable law, including providing access to all data elements of a patient’s electronic health record to the extent permissible under applicable privacy laws

(v) has successfully tested the real world use of the technology for interoperability (as defined in section 3000) in the type of setting in which such technology would be marketed

“Gag clauses”, APIs, “without special effort,” “all data elements,” “such technology (CHIT only?),” real world tests - aligns with current ambulatory EMR focus on APIs but questions re: other products (what is scope of “such technology”) and how to be implemented. Need to do real-world tests.
SEC. 4002. TRANSPARENT REPORTING ON USABILITY, SECURITY, AND FUNCTIONALITY: Enhancements to Certification

- (D) CONDITIONS OF CERTIFICATION.— (Continued)
- (vi) provides to the Secretary an attestation that the developer—
  - (I) has not engaged in any of the conduct described in clause (i)
  - (II) has provided assurances in accordance with clause (ii)
  - (III) does not prohibit or restrict communication as described in clause (iii)
  - (IV) has published information in accordance with clause (iv)
  - (V) ensures that its technology allows for health information to be exchanged, accessed, and used, in the manner described in clause (iv); and
  - (VI) has undertaken real world testing as described in clause (v); and
  - (vii) submits reporting criteria in accordance with section 3009A(b) (transparent reporting about EHRs)
SEC. 4002. TRANSPARENT REPORTING ON USABILITY, SECURITY, AND FUNCTIONALITY

**COMPLIANCE WITH CONDITIONS OF CERTIFICATION.**—The Secretary *may encourage* compliance with the conditions of certification described in subparagraph (D) (Conditions of Certification) and *take action to discourage noncompliance*, as appropriate.
ONC Information Blocking Report

“. . . certain business, technical, and organizational practices are inherently likely to interfere with the exchange of electronic health information in ways that raise these serious information blocking concerns. These practices include but are not limited to:

• Contract terms, policies, or other business or organizational practices that restrict individuals’ access to their electronic health information or restrict the exchange or use of that information for treatment and other permitted purposes.

• **Charging prices or fees** (such as for data exchange, portability, and interfaces) that make exchanging and using electronic health information **cost prohibitive**.

• Developing or implementing health IT in **non-standard ways** that are likely to substantially increase the costs, complexity, or burden of sharing electronic health information, especially when relevant interoperability standards have been adopted by the Secretary.

• Developing or implementing health IT in ways that are likely to “lock in” users or electronic health information; lead to fraud, waste, or abuse; **or impede innovations and advancements** in health information exchange and health IT-enabled care delivery.

Many concepts in ONC report are in (or implied in) Cures (e.g., focus on pricing, “non-standard” implementation, “lock-in”)
ONC Information Blocking Report

**No Reasonable Justification.** Not all conduct that knowingly interferes with electronic health information exchange is information blocking. Accusations of information blocking are serious and should be reserved for conduct that is objectively unreasonable in light of public policy.\textsuperscript{17} Conduct that is required to comply with federal or state privacy law would not be “unreasonable” and would not constitute information blocking under these criteria. Public policy must be balanced to advance important interests, including furthering the availability of electronic health information as needed for authorized and important purposes; protecting and promoting patient safety; maintaining the privacy and security of electronic health information; and protecting the legitimate economic interests and incentives of providers, developers, and other market participants to innovate and compete in ways that ultimately enhance technology, health care, and consumer health and welfare. (pp 11-12)

“Reasonableness” will be critical to how this concept is implemented and enforced. ONC recognizes “legitimate economic interests and incentives of developers to innovate and compete“.
Whether any reasonable justification exists will depend on the attendant facts and circumstances and require a careful consideration of the objective reasons for the practice; its likely impact on health information exchange; the extent to which it could have been reasonably avoided; and the extent to which it advances any countervailing interest.

The HITECH Act recognizes the need to protect the legitimate economic interests of . . . Developers [which] provide incentives to innovate and compete to improve health care and health IT . . . developers who invest resources to develop and deploy more effective, interoperable health IT and health information exchange capabilities may not do so if they cannot realize a return on their investments. In addition, competition among developers . . . may reduce the costs of these technologies and provide more options for those who purchase and use them. On the other hand, . . . At some point, . . . decisions to engage in such practices are unreasonable as against public policy, particularly when less restrictive alternatives exist and the economic benefits to consumers are outweighed by the costs to consumers of less effective and efficient health care. (pp. 13-14)

Note emphasis on specific facts and circumstances, need for reasonable return on developer investments, and existence of competition and alternatives.
Identifying information blocking is a difficult and highly fact-specific task that requires access to detailed and often sensitive information about provider or developer business, technical, and organizational practices. For example, where a developer engages in pricing or contractual practices that interfere with the exchange or use of electronic health information, evidence as to the developer’s actual costs, prices, business model, and technology design decisions is necessary to determine whether the interference has any reasonable justification, and thus whether it rises to the level of information blocking. (p. 29)
Reasonable and Necessary: Vendor Community Perspectives

- Potential categories of “reasonable and necessary:
  - Privacy protections
  - Data security
  - System performance
  - Use of non-standard applications
  - Network participation
  - Fees
  - Other agreements and terms of use that enable, expand, and enhance information sharing
Attestations (MU & ACI) - Information Blocking & Connectivity Per MACRA

1. Did not knowingly and willfully take action (e.g., disable functionality) to limit or restrict compatibility or interoperability of CEHRT.

2. Implemented technologies, standards, policies, practices, and agreements reasonably calculated to ensure, to the greatest extent practicable and permitted by law, that CEHRT was, at all relevant times: connected in accordance with applicable law; compliant with all standards applicable to exchange of information, including ONC standards, implementation specifications, and certification criteria; implemented in a manner that allowed for timely, secure, and trusted bi-directional exchange of structured electronic health information with other providers, including unaffiliated providers, and with disparate CEHRT and vendors.

3. Responded in good faith and in a timely manner to requests to retrieve or exchange electronic health information, including from patients, health care providers, and other persons, regardless of requestor’s affiliation.

Finalized as proposed, with CMS indicating overall “good faith” standard and extensive responses to comments that appear to provide some flexibility.
OIG Enforcement Status

- At HIMSS17, OIG indicated that they would not engage in active enforcement pending needed regulatory clarity on “reasonable and necessary”
- Position reinforced at October 2017 Senate HELP hearing
Regulatory Status

- ONC and OIG engaged in discussions with stakeholders
- ONC to address “reasonable and necessary” and developer certification implications as part of April 2018 “Cures” proposed rule
- OIG enforcement to follow
- Trusted Exchange Framework and Common Agreement (TEFCA) could interrelate with Information Blocking
  - Some commenters have called for a TEFCA safe harbor
What Should I Do Now?

- Review the statute
- Develop initial compliance strategy
- Review/comment on April ONC proposed rule
- Adjust compliance strategy for proposed and final rule

Thank you!

Mark J. Segal, PhD, FHIMSS
Principal, Digital Health Policy Advisors, LLC
Chair, HL7 Policy Advisory Committee

msegal@dig-hpa.com