Identifying and Remediating Information Blocking Practices

Presentation to Massachusetts Health Data Consortium

February 23, 2020

DAVIS WRIGHT TREMAINE LLP
Adam Greene, Partner
Agenda

1. Why Is This Important?
2. How We Got Here
3. Information Blocking – The Big Picture
4. Key Concepts
5. Exceptions
6. How to Tackle Information Blocking
7. Takeaways
Hi, I’m conducting a quality assessment study for The King’s Hospital. Attached is a list of all 2021 Admissions to The King’s Hospital, including patient names, DOBs, and discharge dates. Please match this to your patient list and provide me with assessment, clinical notes, and procedure information for each encounter within 90 days of our discharge dates. Call me if you have any questions. Thank you for your assistance.
Why Is This Important?
I’m just following up on the below email:

Hi, I’m conducting a quality assessment study for The King’s Hospital. Attached is a list of all 2021 admissions to The King’s Hospital, including patient names, DOB’s, and discharge dates. Please match this to your patient list and provide me with assessment, clinical notes, and procedure information for each encounter within 90 days of our discharge dates. Call me if you have any questions. Thank you for your assistance.
Why Is This Important?
Why Is This Important?

Report Information Blocking

In your submission, please consider including information that will help us understand the concern(s) you are reporting. Examples of information that would be particularly helpful would include, but not be limited to:

- Person or entity that requested access, exchange, or use of electronic health information (EHI)
  - Role of person/entity (e.g., patient, health care provider, health information network/exchange (HIN/HE), health IT developer of certified health IT)
  - Date and time of request
  - Location of requestor (city, state)
- Type of EHI requested (e.g., lab result, medical history, diagnostic images)
- Type/purpose of request (e.g., patient request to access his/her records; health care provider request to export patient records from a different health care provider)
- Health IT being used by the requestor (e.g., system and version)
- Person or entity that denied did not fulfill the request to access, exchange, or use EHI
  - Role of person/entity (e.g., health care provider, HIN/HE, health IT developer of certified health IT)
  - Date and time the request was denied/not fulfilled
  - Location of person/entity (city, state)

If you have any technical questions, please reach out to omh-hta-questions@healthit.gov.
Any action – or inaction – that knowingly “interferes” with access, exchange or use of electronic health information ("EHI") may lead to various disincentives or penalties.
Why Is This Important?

Ignoring the request could represent information blocking, resulting in:

- Disincentives (of a type that are not yet known) for information blocking as a health care provider; and
  - Decrease in Medicare reimbursement (if provider attests that it is information blocking as part of the Meaningful Use program); and
  - Identification on a CMS website as attesting to information blocking; or
  - False claims act liability if provider inaccurately attests to not information blocking
How We Got Here

Silo of paper medical records

Billions spent on EMRs

ONC Report to Congress on InfoBlocking (4/15)

MACRA* adds InfoBlocking (4/15)

21st Century Cures Act (12/16)

MACRA regs add InfoBlocking attestations (11/16)

MACRA InfoBlocking attestations implemented (CY17)

ONC Proposed Cures Act Rule (3/19)

OIG Proposed Enforcement Rule (4/20)

ONC Final Cures Act Rule (5/20)

Extension of Compliance Dates (11/20)

* Medicare Access and CHIP Reauthorization Act of 2015
The Puzzle

Two Different Information Blocking Standards

MACRA
- Three attestations as part of Promoting Interoperability performance criteria (aka Meaningful Use)
- In effect since CY2017 meaningful use reporting period
- Attestations will be publicized on CMS website in the future

Cures Act
- New definition of information blocking
- Governs broader set of “actors” and different penalties
MACRA – Info Blocking

Three attestations:

1. Did not take action to limit or restrict the compatibility or interoperability of certified EHR technology

2. Implemented certified EHR technology so that it is connected, compliant with applicable standards, and allows patient access and bi-directional exchange with unaffiliated health care providers

3. Respond in good faith to requests to exchange electronic health information
Cures Act – Information Blocking Definition

Except if:

- Practice is required by law
- Falls under HHS rulemaking exception
- Practice is likely to ...

Interfere with, prevent, or materially discourage ...
21st Century Cures Act

Information Blocking Definition (Translation)

- Access, exchange, or use ...
- Electronic Health Information
- Knowledge
  - Knows or Should Know (health information technology developer, exchange, or network); or
  - Knows practice is unreasonable (health care provider)
Information Blocking – Actors

- Health Care Providers
- Health IT Developers of Certified Health IT
- Health Information Networks (HIN) / Health Information Exchanges (HIE)
IB Actors – Health Care Providers

A health care provider is a: 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 Indian Health Service or by an Indian tribe, tribal organization, or urban Indian organization; rural health clinic; covered entity under 42 U.S.C. 256b; therapist; and any other category of health care facility, entity, practitioner, or clinician determined appropriate by the HHS Secretary.*

* See full definition of “Health Care Provider” at 42 U.S.C. 300jj.
Controls or discretion to administer, permit, enable, or require the use of any technology or services for access, exchange, or use of EHI:

1. Among *more than two* unaffiliated individuals or entities; and

2. That is for a treatment, payment, or health care operations purpose.
IB Actors – Health IT Developer of Certified IT

- An individual or entity that develops or offers health IT (e.g., EHR Community Connect); and

- At the time it engages in a practice that is subject of an information blocking claim, has one or more health IT modules certified or recognized by the ONC Health IT Certification Program.

Note: Excludes health care providers that self-develop health IT for its own use.
Information Blocking – EHI Defined

- Electronic Health Information (“EHI”) is defined as:
  - Electronic protected health information (ePHI, as defined under HIPAA, 45 CFR 160.103),
  - To the extent that ePHI would be included in a designated record set (even if for non-HIPAA covered entity)
    - Medical records
    - Billing records
    - Other records used to make decisions about individuals
Information Blocking – EHI Defined

What is not “EHI”?

► Psychotherapy notes

► Information compiled in reasonable anticipation of, or for use in, civil, criminal, or administrative actions.

► Information that falls outside of a designated record set, such as:
  – De-identified information
  – ePHI that is used for internal quality improvement, business analytics, or otherwise is not used to make health care decisions about individuals.
Information Blocking – EHI

“EHI” Limited Further for the first 24 Months (through October 5, 2022)

- "EHI" is further limited to just the data elements represented in the USCDI standard adopted in 45 CFR 170.213.

- The United States Core Data for Interoperability (USCDI) is a standardized set of health data classes and constituent data elements for nationwide, interoperable health information exchange.

- Current version: USCDI v.1 (Errata July 2020)

Full “EHI” definition goes into effect October 6, 2022
Q. Do the information blocking requestions ... require actors to proactively make [EHI] available through “patient portals,” [APIs], or other health information technology?

No. There is no requirement under the information blocking regulations to proactively make available any EHI to patients or others who have not requested the EHI. We note, however, that a delay in the release or availability of EHI in response to a request for legally permissible access, exchange, or use of EHI may be an interference under the information blocking regulations (85 FR 25813, 25878). If the delay were to constitute an interference under the information blocking regulations, an actor’s practice or actions may still satisfy the conditions of an exception under the information blocking regulations (45 CFR 171.200-303).
Information Blocking Penalties

- Civil monetary penalties up to $1 million per violation for:
  - Health IT developers of certified health IT
  - HIEs/HINs

- Health care providers “appropriate disincentives” that fall under existing authority – awaiting rulemaking
Information Blocking Timeline

- Compliance date for Cures Act information blocking rule is April 5, 2021
- Enforcement date?
  - For Health IT developers and HIE/HINs, likely 60 days after OIG rule is finalized
  - For health care providers, no proposed enforcement rule yet
- MACRA attestations continue
Eight Exceptions

HHS Office of the National Coordinator of Health IT, https://www.healthit.gov/topic/information-blocking
Exceptions Overview

- A practice that does NOT meet all the conditions of an exception will not automatically constitute Information Blocking.

- But, if there is an Information Blocking complaint filed, and an investigation is opened:
  - No guaranteed protection from penalties under the information blocking regulations, and
  - Scrutiny of the facts and circumstances surrounding at least one of your practices.
Preventing Harm Exception

- Protecting patients and other persons against unreasonable risks of harm can justify practices that interfere with access, exchange, or use of EHI

- Harm standard: generally life or physical safety of an individual

- Must hold a reasonable belief the practice will substantially reduce the risk of harm
Privacy Exception

- May comply with patients’ privacy requests
- Must comply with privacy law requirements
- If privacy laws permits disclosure, must disclose (unless another exception applies)
Security Exception

Covers practices implemented to safeguard the confidentiality, integrity, and availability of EHI

Must be tailored to specific security risks

Implemented in a consistent and non-discriminatory way
Health IT Performance Exception

- Recognizes that health IT must be maintained and improved from time to time to perform properly
- May degrade or take health IT temporarily offline to implement performance enhancements
- E.g., provider’s planned EHR upgrade
Infeasibility Exception

- Legitimate practical challenges may limit others’ access, exchange, or use of your EHI
- Examples: technological capabilities, legal rights, uncontrollable events
- Must provide written response within 10 business days with reason(s) request is infeasible
Content and Manner Exception

- Addresses technical formatting and EHI transport issues
- Generally must provide EHI in the manner requested, unless:
  - Technically unable to fulfill the request
  - Cannot reach agreeable terms with requestor
- If cannot provide EHI in the manner requested:
  - May send in another machine-readable format
Fees Exception

- Allows you to charge fees for access, exchange, or use of EHI
- Fees must be cost-based and non-discriminatory
- Two types of fees will be particularly scrutinized:
  1. Fees for electronic access to EHI
  2. Fees for export of EHI tied to an individual or clinician
Licensing Exception

- Allows actors to protect the value of their Health IT innovation(s)
- May charge reasonable royalties to earn ROIs in developing, maintaining, and updating those innovations
- Licensing conditions: non-discriminatory and more “fair”
How to Tackle Info Blocking
Develop a Process

- Learn about Info Blocking
- Convene Relevant Stakeholders
- When Are You an Info Blocking “Actor”?

- Draft (or revise) Info Blocking policies
- Train on Info Blocking Policies
- Assess Compliance
- Remediate Info Blocking Practices
- Identify Info Blocking Practices
Learn About Info Blocking

Congratulations, you’re doing that now!

Other resources:

- The ONC Rule at https://www.healthit.gov/curesrule/download
- The ONC website at https://www.healthit.gov/topic/information-blocking
Convene Relevant Stakeholders

- Privacy/Compliance
- Legal/Contracting
- Health Information Management
- EHR/Patient Portal Team
- Security
When Are You an Info Blocking “Actor”

▶ Are you a health care provider?

➢ Yes.

▶ Are you a health IT developer of certified health IT?

➢ Likely no, unless you offer certified EHR to others.

▶ Are you a health information network or health information exchange?

➢ Likely no, unless you facilitate exchange of EHI to three or more unaffiliated providers.
Draft Policies

- Prohibition of information blocking.
- Who is responsible?
- Procedure for reporting potential information blocking practices.
- Procedure for auditing.
- Procedure for attesting to no information blocking.
Conduct Training

- What is information blocking?
- Who handles requests for EHI?
- What are the exceptions?
- To whom do you internally report potential information blocking practices?
Identify Information Blocking Practices

What systems involve requests and/or disclosures of EHI?

- Health information management
- Patient portal
- Contracting with third parties

DWT Information Blocking Toolkit, © 2020 Davis Wright Tremaine LLP
Identify Information Blocking Practices

For each system, what practices interfere with access, exchange, and use of EHI?

- Denial of requests to share patients’ EHR with other providers?
- Intentional delays in providing lab results to patients?
- Potentially unreasonable security practices?
- Restrictive contract terms?
Identify Information Blocking Practices

For each practice that raises an issue:

- Does it involve EHI?
- Is it required by law?
- Does at least one of the 8 exceptions apply?
- Are all of the exception’s criteria met?
Information Blocking Risks

- You may be at risk of violating the information blocking regulations if you have a practice that:
  - Meets the elements of information blocking; and
  - Does not meet an exception.

- If subjected to an information blocking investigation, these practices will be analyzed on a case-by-case basis to evaluate the facts and circumstances on which that practice is based on
Remediate Potential Information Blocking Practices

- Modify your practice to bring it within one of the exceptions
- If unable to bring it within an exception, then maintain documentation on your practice that includes:
  - A description of the facts and circumstances of the practice;
  - Why you engaged in the practice; and
  - Why you determined the practice is “reasonable and necessary.”
Takeaways
Takeaways

- We got a stay of execution, but April 5, 2021 will be here before you know it.
  - Convene stakeholders
  - Identify information systems
  - Assess practices within those information systems
  - Check each practice against the Exceptions
  - Remediate practices that are not “reasonable and necessary”
Questions?
Adam H. Greene
Partner | D.C.
202.973.4213
adamgreene@dwt.com

Adam’s practice focuses on health information privacy and security laws, using his experience as a former regulator to help clients understand how they can permissibly leverage their health data, bring their information security programs into compliance with the HIPAA Security Rule, and respond to potential breach incidents. He works with healthcare providers, health plans, cloud services providers, health IT companies, and financial institutions to navigate HIPAA and the patchwork of other federal and state health information laws.