How New Regulations on Information Blocking Change Everything About Managing Patient Information

September 15, 2020

DAVIS WRIGHT TREMAINE LLP

Adam H. Greene, Partner

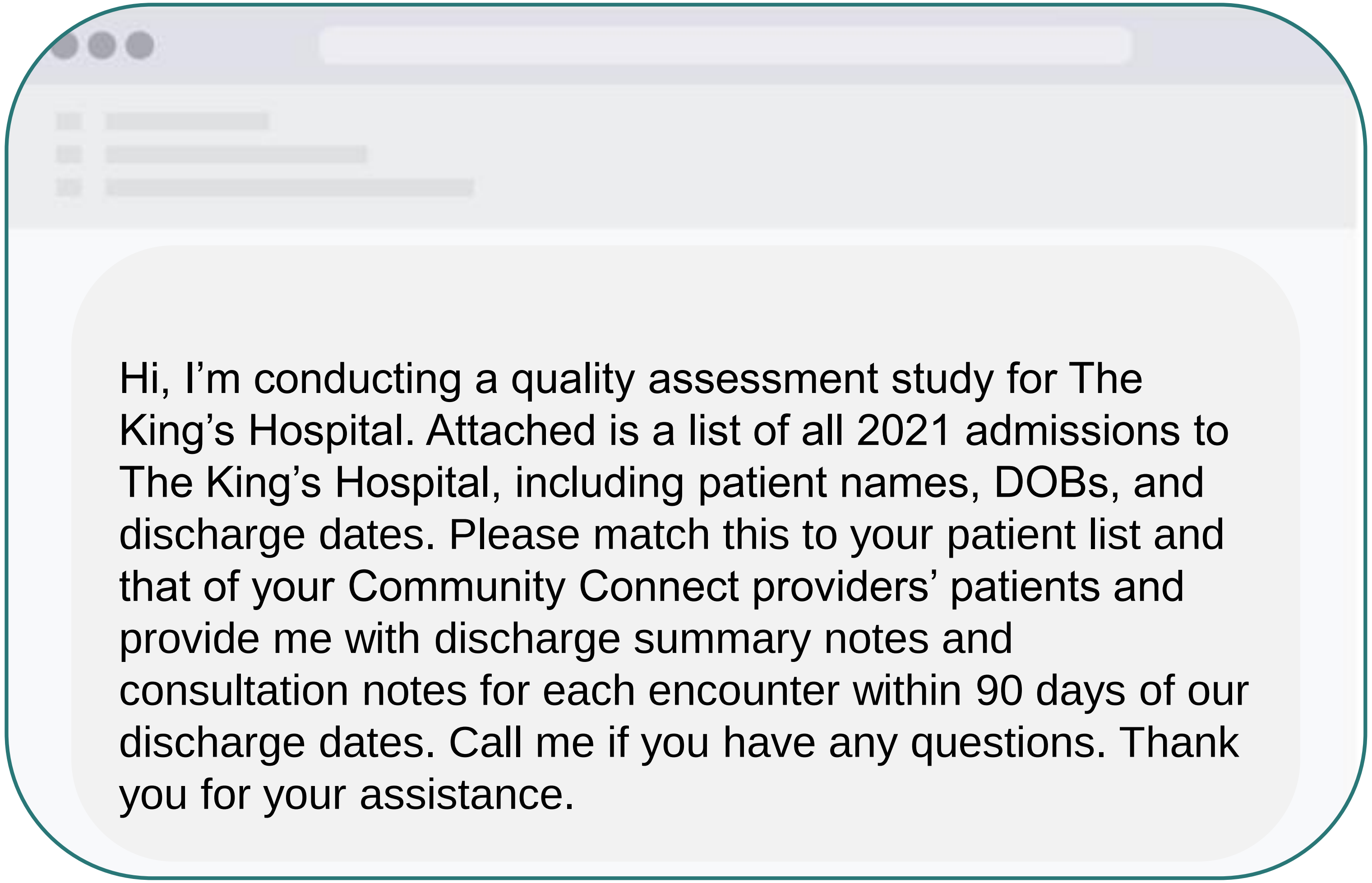
Michaela B. Andrawis, Associate

Davis Wright Tremaine LLP

Agenda

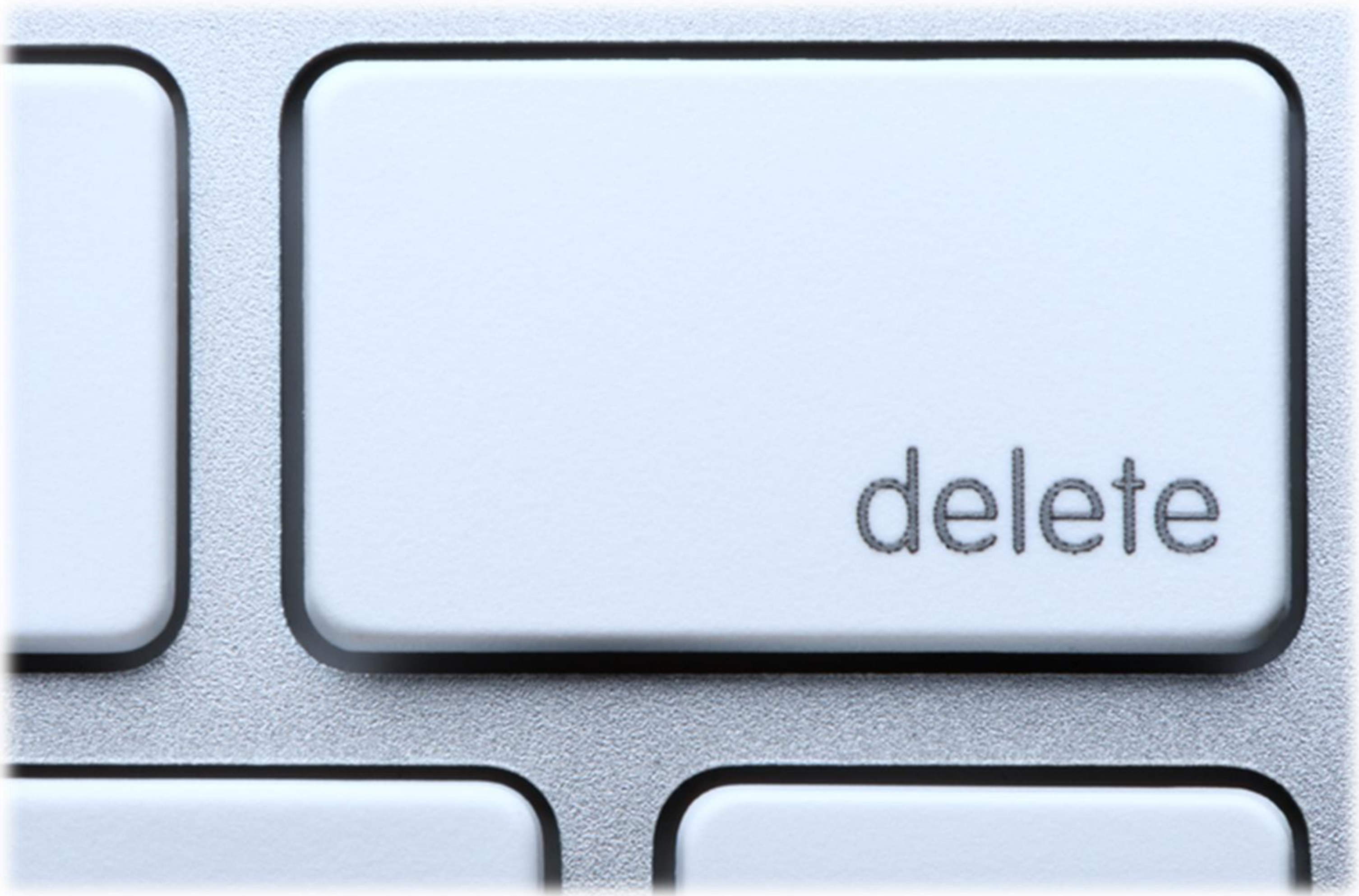
1. Why Is This Important?
2. How We Got Here
3. Information Blocking – The Big Picture
4. Key Concepts
5. Exceptions
6. How to Tackle Information Blocking
7. Takeaways

Why Is This Important?

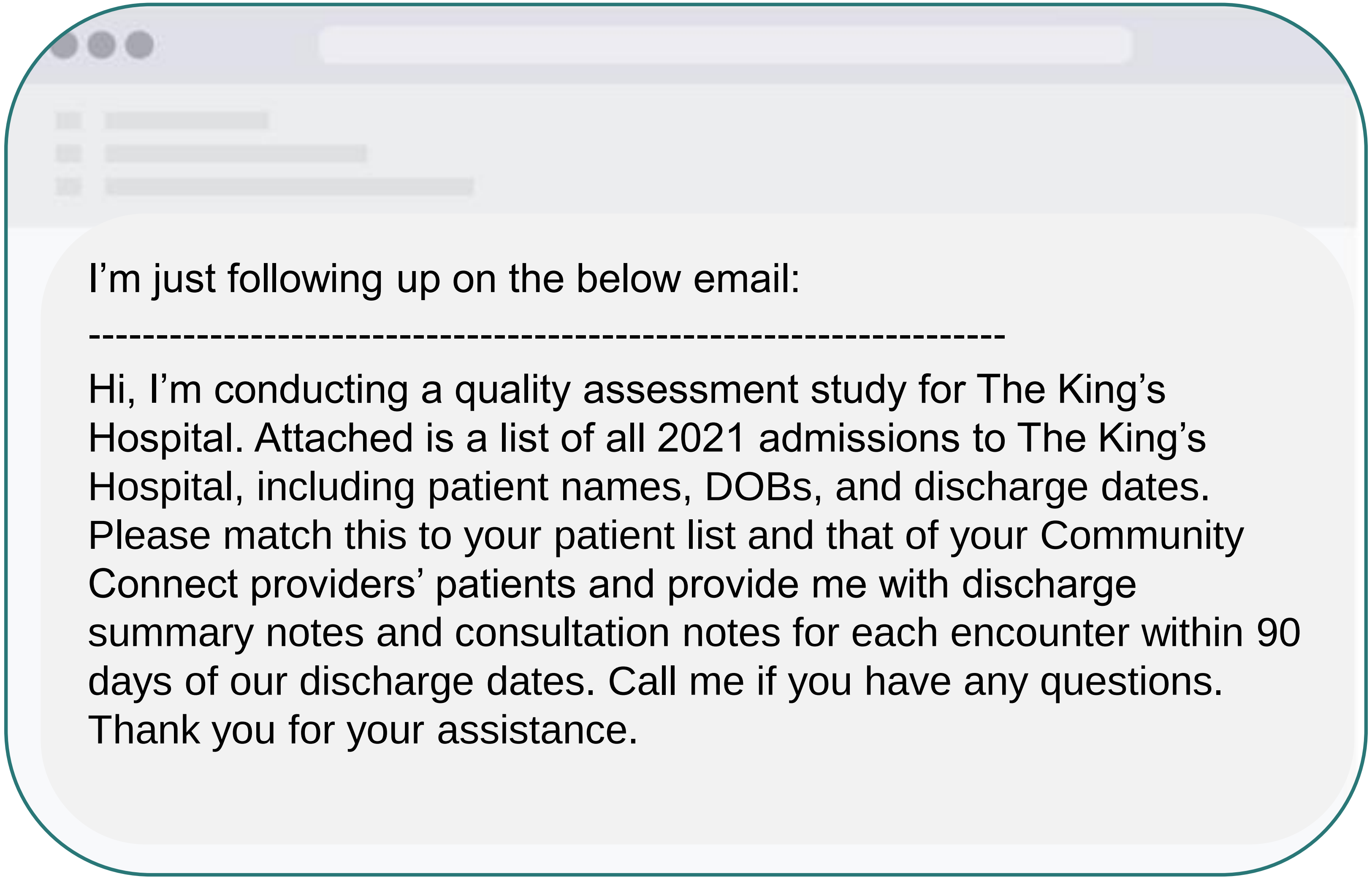


Hi, I’m conducting a quality assessment study for The King’s Hospital. Attached is a list of all 2021 admissions to The King’s Hospital, including patient names, DOBs, and discharge dates. Please match this to your patient list and that of your Community Connect providers’ patients and provide me with discharge summary notes and consultation notes 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?



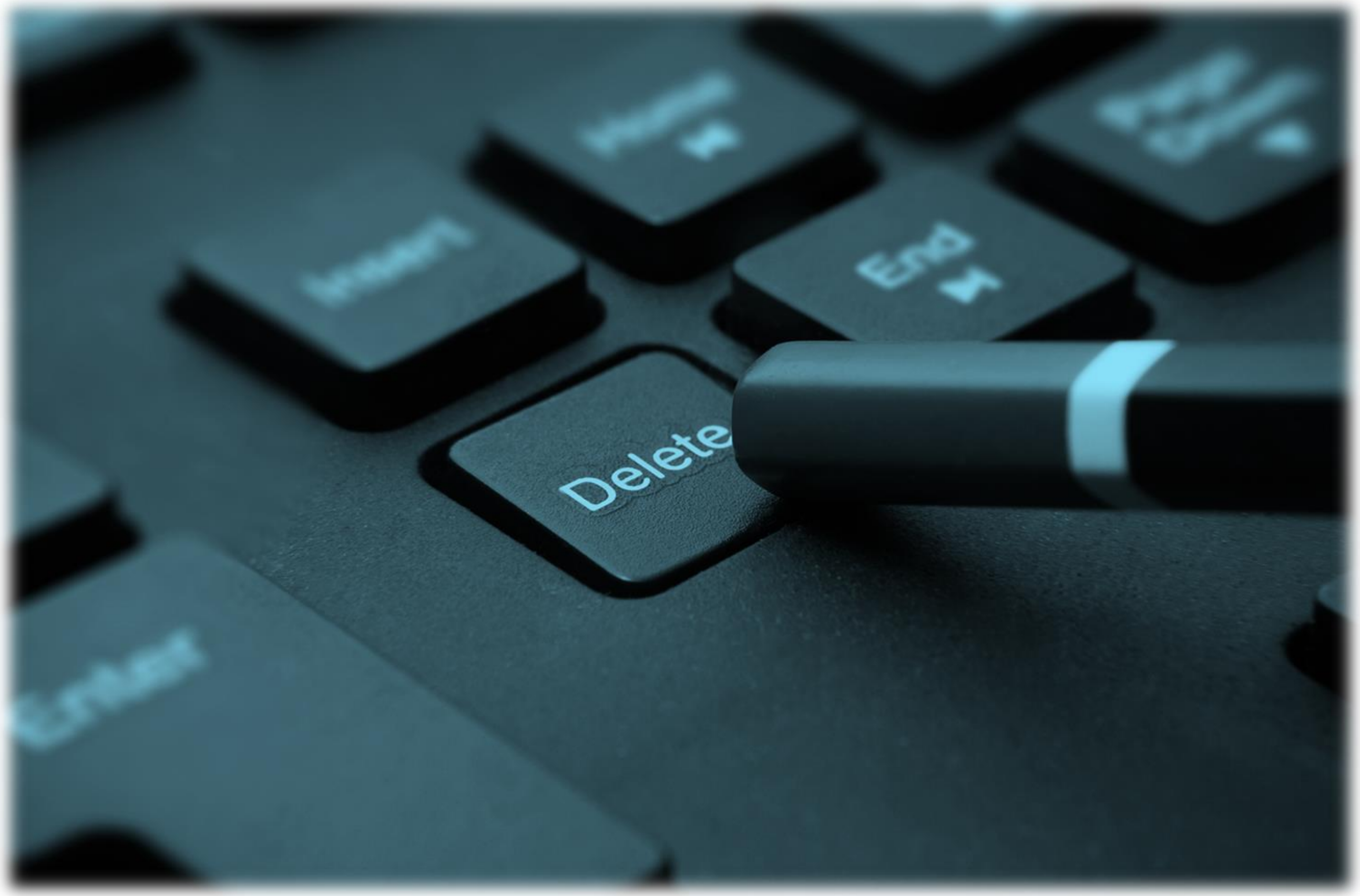
Why Is This Important?



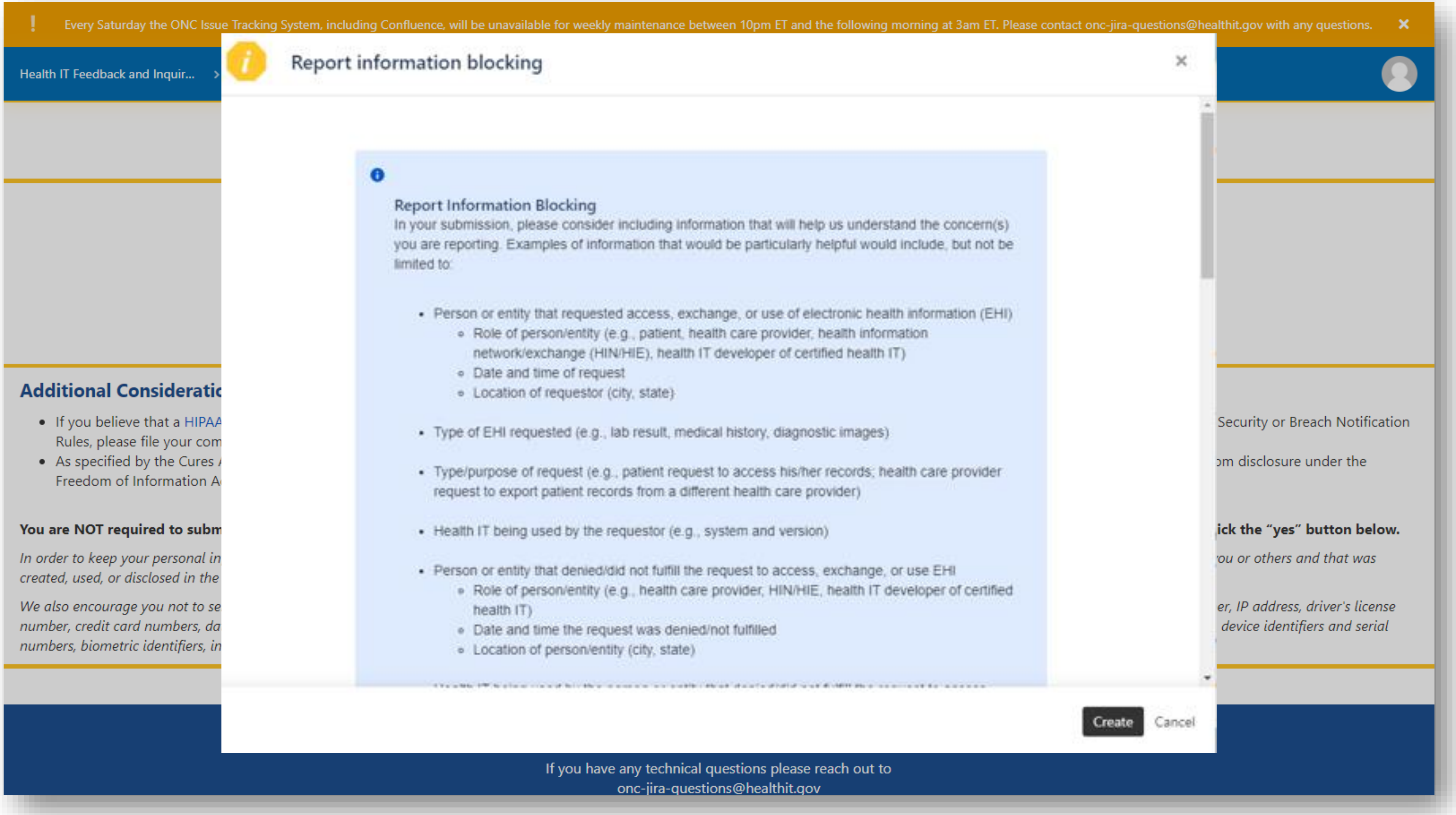
I’m just following up on the below email:

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, DOBs, and discharge dates. Please match this to your patient list and that of your Community Connect providers’ patients and provide me with discharge summary notes and consultation notes 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?



Every Saturday the ONC Issue Tracking System, including Confluence, will be unavailable for weekly maintenance between 10pm ET and the following morning at 3am ET. Please contact onc-jira-questions@healthit.gov with any questions.

Report information blocking

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/HIE), 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/HIE, health IT developer of certified health IT)
  - Date and time the request was denied/not fulfilled
  - Location of person/entity (city, state)

Additional Consideratic

- If you believe that a HIPAA ... Security or Breach Notification Rules, please file your com...
- As specified by the Cures ... om disclosure under the Freedom of Information A...

You are NOT required to subm ... ick the "yes" button below.

In order to keep your personal in ... ou or others and that was created, used, or disclosed in the ...

We also encourage you not to se ... er, IP address, driver's license number, credit card numbers, da ... device identifiers and serial numbers, biometric identifiers, in...

If you have any technical questions please reach out to onc-jira-questions@healthit.gov

Why Is This Important?

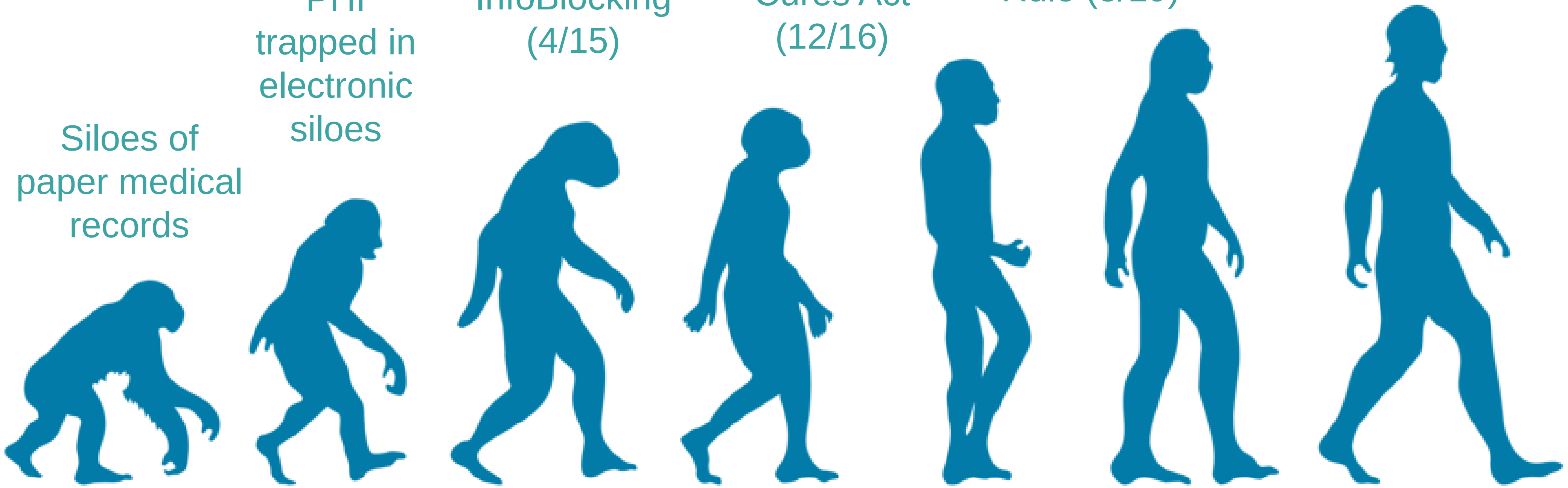
Any action – or inaction – that knowingly "interferes" with access, exchange or use of electronic health information ("EHI") may lead to various disincentives or penalties.

Why Is This Important?

Ignoring the request could represent information blocking, resulting in:

- $1 million penalty (with respect to withholding the electronic health information of the Community Connect providers);
- 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



Siloes of paper medical records

Billions spent on EMRs

PHI trapped in electronic siloes

ONC Report to Congress on InfoBlocking (4/15)

MACRA adds InfoBlocking (4/15)

MACRA regs add InfoBlocking attestations (11/16)

21st Century Cures Act (12/16)

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)

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

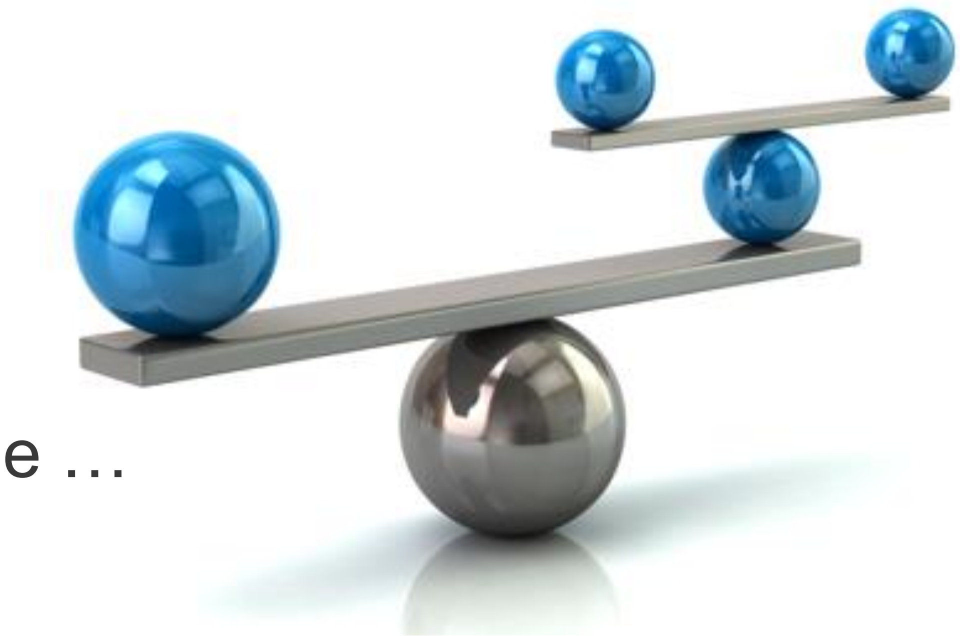
MACRA – Info Blocking

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 <u>required by law</u>
  - Falls under HHS <u>rulemaking exception</u>
- Practice is <u>likely</u> to …
- <u>Interfere</u> 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
(including Hospitals)

Health IT
Developers of
Certified Health IT

Health Information
Networks (HIN)/
Health Information
Exchanges (HIE)

IB Actors – Health Care Providers

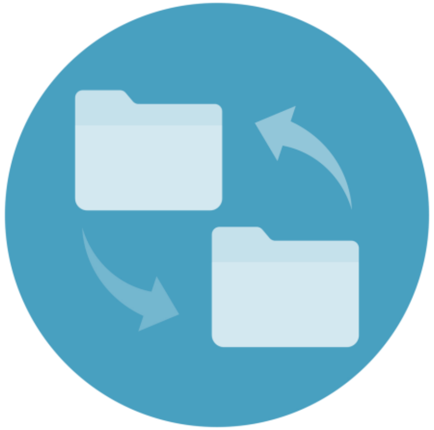
- A health care provider is a: hospital; skilled nursing facility; nursing facility; home health entity or other long term care facility; health care clinic; community mental health center; renal dialysis facility; blood center; ambulatory surgical center; emergency medical services provider; federally 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.

IB Actors – HIN/ HIEs

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 <u>designated record set</u> (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"?

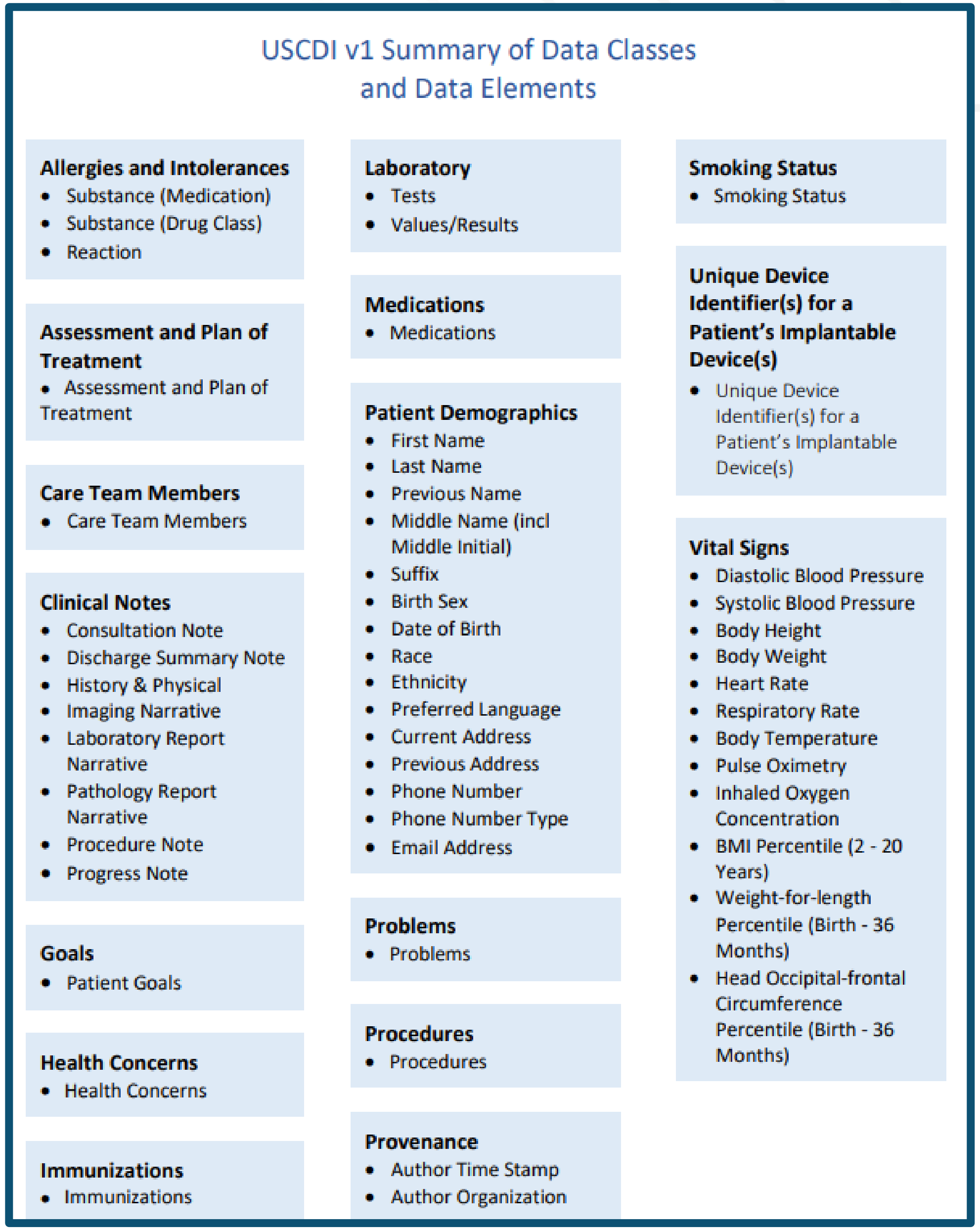
- Psychotherapy notes
- Information compiled in reasonable anticipation of, or for use in, civil, criminal, or administrative actions.
- Information that falls outside of a designated record set, such as:
  - De-identified information
  - ePHI that is used for internal quality improvement, business analytics, or otherwise is not used to make health care decisions about individuals.

Information Blocking - EHI

“EHI” Limited Further for the first 24 Months (through May 1, 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 May 2, 2022



USCDI v1 Summary of Data Classes
and Data Elements

Allergies and Intolerances
- Substance (Medication)
- Substance (Drug Class)
- Reaction

Assessment and Plan of Treatment
- Assessment and Plan of Treatment

Care Team Members
- Care Team Members

Clinical Notes
- Consultation Note
- Discharge Summary Note
- History & Physical
- Imaging Narrative
- Laboratory Report Narrative
- Pathology Report Narrative
- Procedure Note
- Progress Note

Goals
- Patient Goals

Health Concerns
- Health Concerns

Immunizations
- Immunizations

Laboratory
- Tests
- Values/Results

Medications
- Medications

Patient Demographics
- First Name
- Last Name
- Previous Name
- Middle Name (incl Middle Initial)
- Suffix
- Birth Sex
- Date of Birth
- Race
- Ethnicity
- Preferred Language
- Current Address
- Previous Address
- Phone Number
- Phone Number Type
- Email Address

Problems
- Problems

Procedures
- Procedures

Provenance
- Author Time Stamp
- Author Organization

Smoking Status
- Smoking Status

Unique Device Identifier(s) for a Patient’s Implantable Device(s)
- Unique Device Identifier(s) for a Patient’s Implantable Device(s)

Vital Signs
- Diastolic Blood Pressure
- Systolic Blood Pressure
- Body Height
- Body Weight
- Heart Rate
- Respiratory Rate
- Body Temperature
- Pulse Oximetry
- Inhaled Oxygen Concentration
- BMI Percentile (2 - 20 Years)
- Weight-for-length Percentile (Birth - 36 Months)
- Head Occipital-frontal Circumference Percentile (Birth - 36 Months)

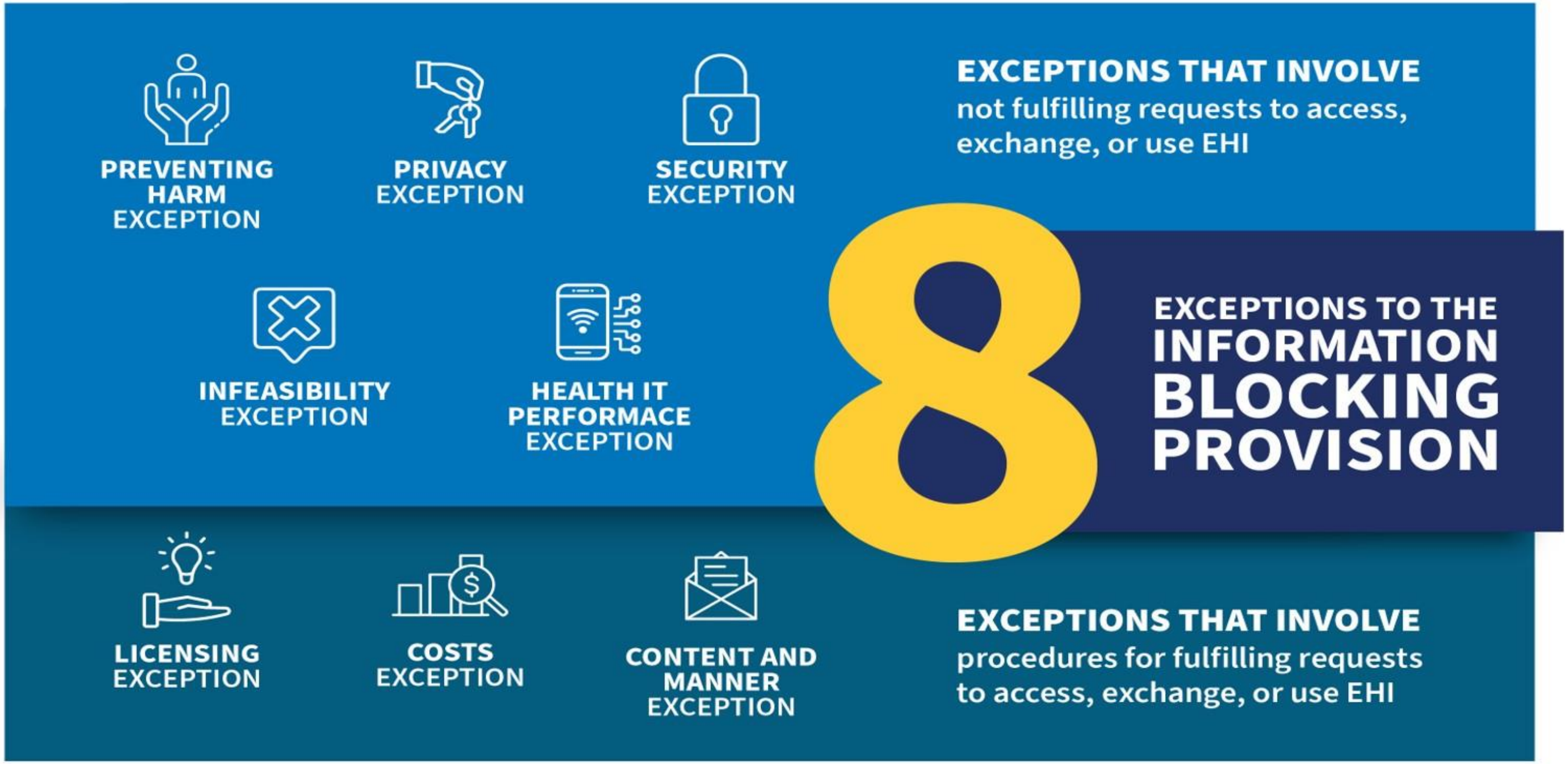
Information Blocking Penalties

- 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 November 2, 2020.
- 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



PREVENTING HARM EXCEPTION

PRIVACY EXCEPTION

SECURITY EXCEPTION

EXCEPTIONS THAT INVOLVE not fulfilling requests to access, exchange, or use EHI

INFEASIBILITY EXCEPTION

HEALTH IT PERFORMACE EXCEPTION

8 EXCEPTIONS TO THE INFORMATION BLOCKING PROVISION

LICENSING EXCEPTION

COSTS EXCEPTION

CONTENT AND MANNER EXCEPTION

EXCEPTIONS THAT INVOLVE procedures for fulfilling requests to access, exchange, or use EHI

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

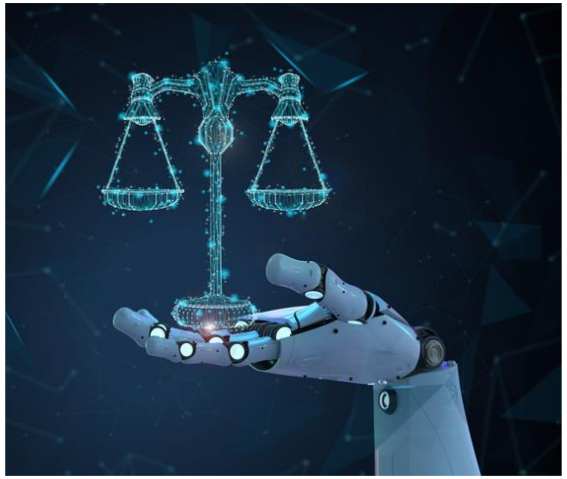
Privacy Exception

- 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 full 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

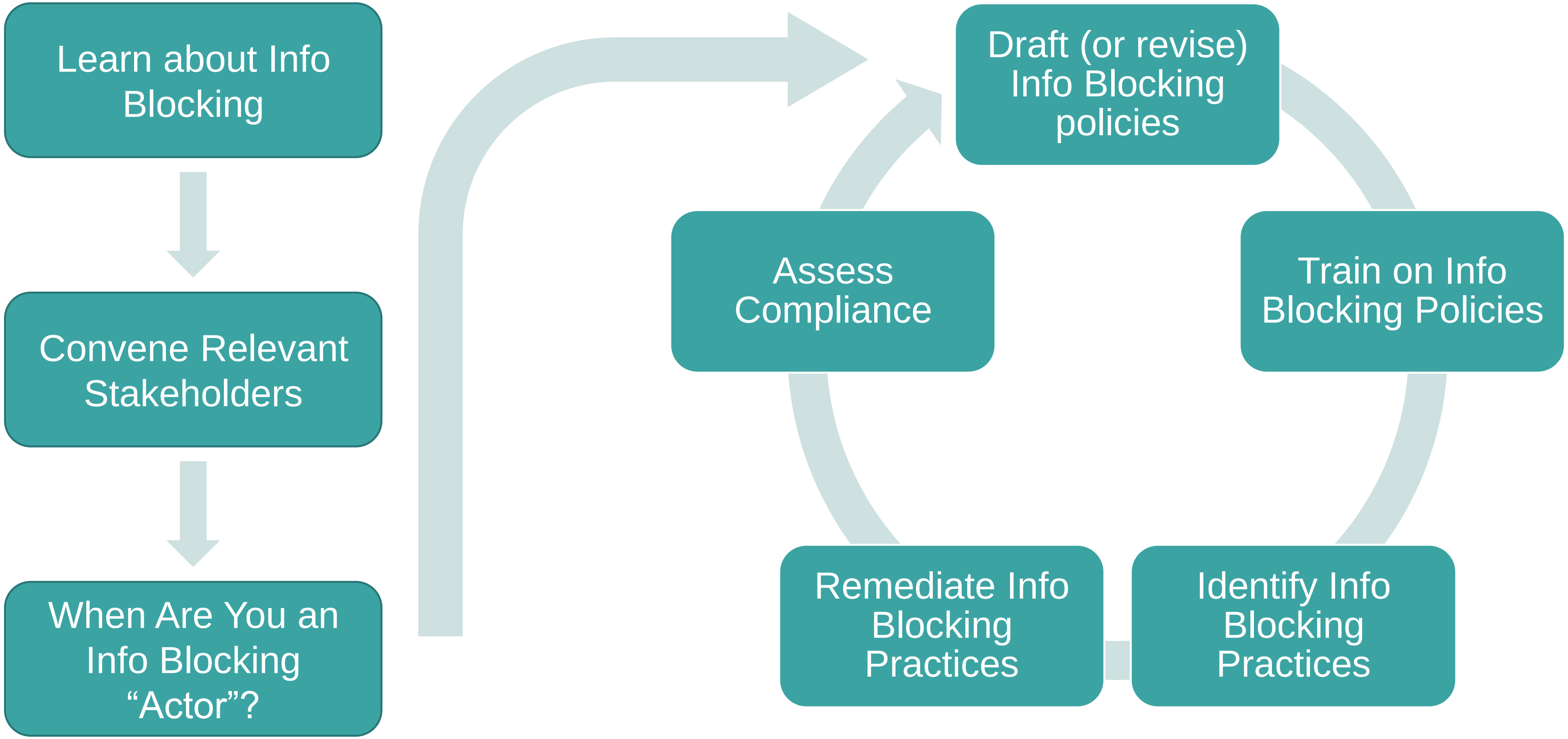
- Allows you to charge fees for access, exchange, or use of EHI
- Fees must be cost-based and non-discriminatory
- Two types of fees with be particularly scrutinized:
    1. Fees for electronic access to EHI
    2. Fees for export of EHI tied to an individual or clinician

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”
  - Assess existing licensing agreements prior to enforcement date
    (November 2nd or later)

How to Tackle Info Blocking in Your Hospital

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
Identify Info Blocking Practices
Remediate Info Blocking Practices
Assess Compliance

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

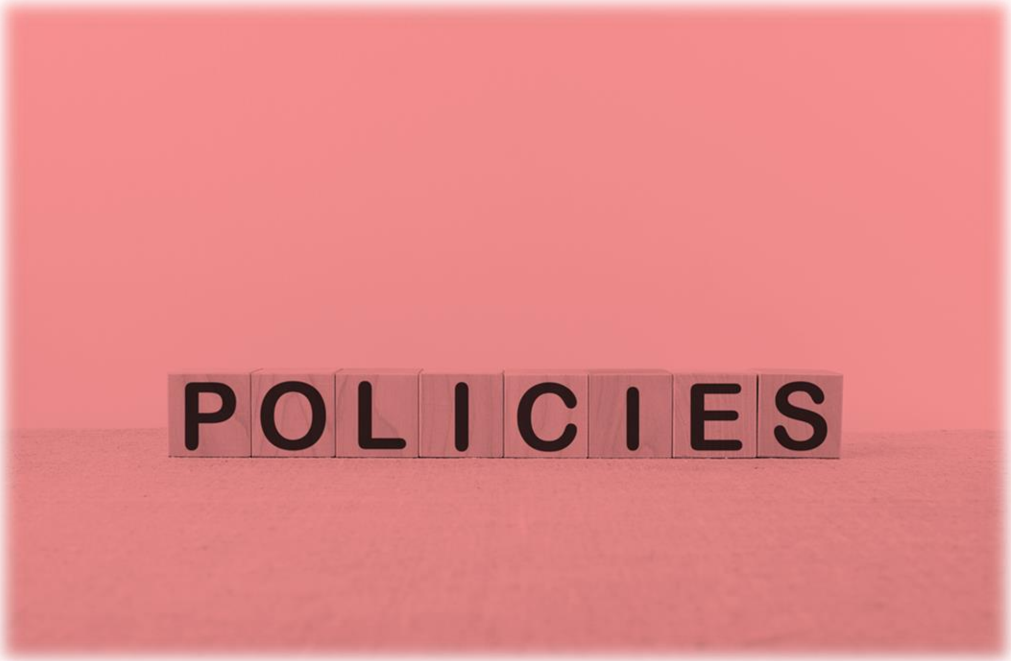
Security

When Are You an Info Blocking “Actor”

- Are you a health care provider?
  - Yes.
- Are you a health IT developer of certified health IT?
  - Yes, if you offer certified EHR to others (e.g., through EHR Community Connect)
- Are you a health information network or health information exchange?
  - Yes, if you facilitate exchange of EHI to three or more unaffiliated providers (e.g., through EHR Community Connect).

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.

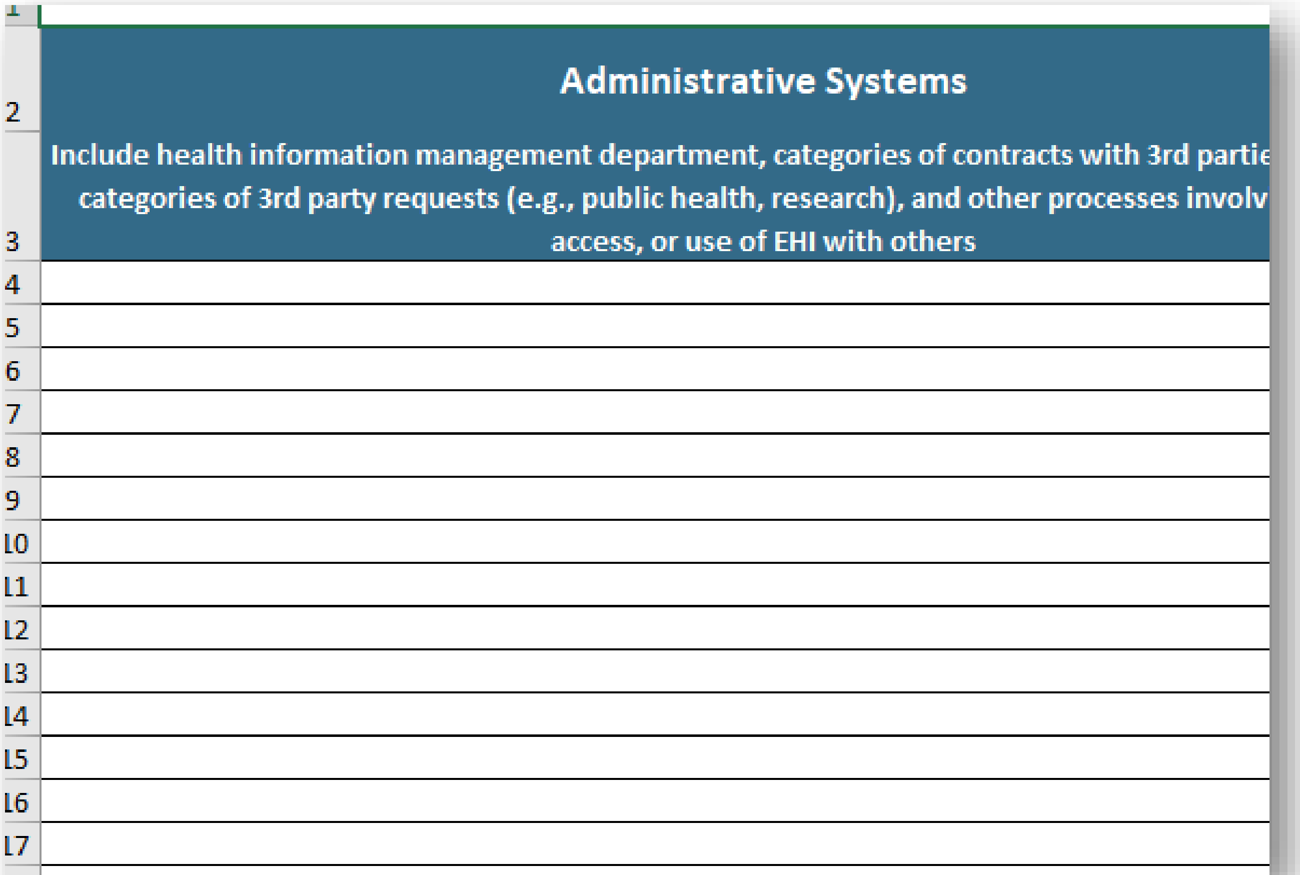


Conduct Training

- 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 department
  - Patient portal
  - Contracting with third parties

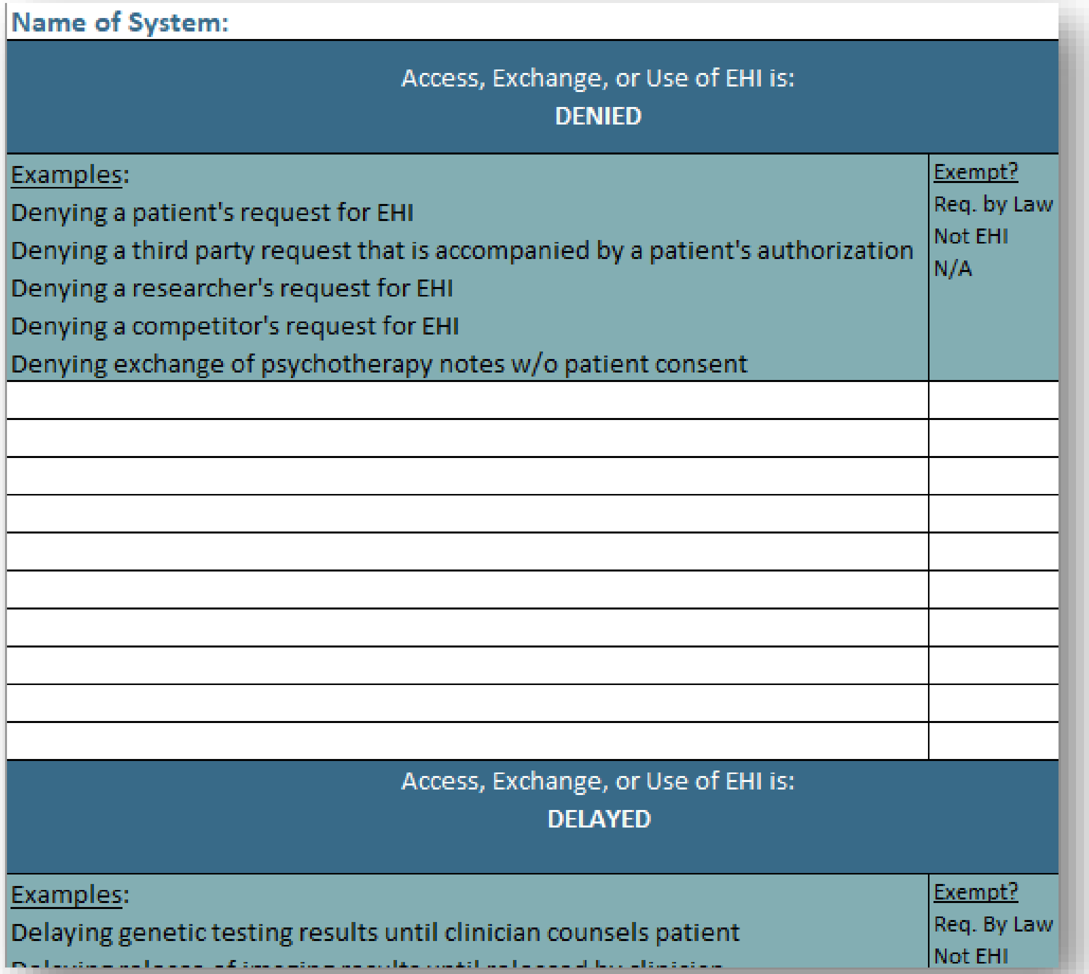


1	
2	**Administrative Systems**
3	Include health information management department, categories of contracts with 3rd partie categories of 3rd party requests (e.g., public health, research), and other processes involv access, or use of EHI with others
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	

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 connect to EHR?
  - Intentional delays in providing lab results to patients?
  - Potentially unreasonable security practices?
  - Restrictive contract terms?

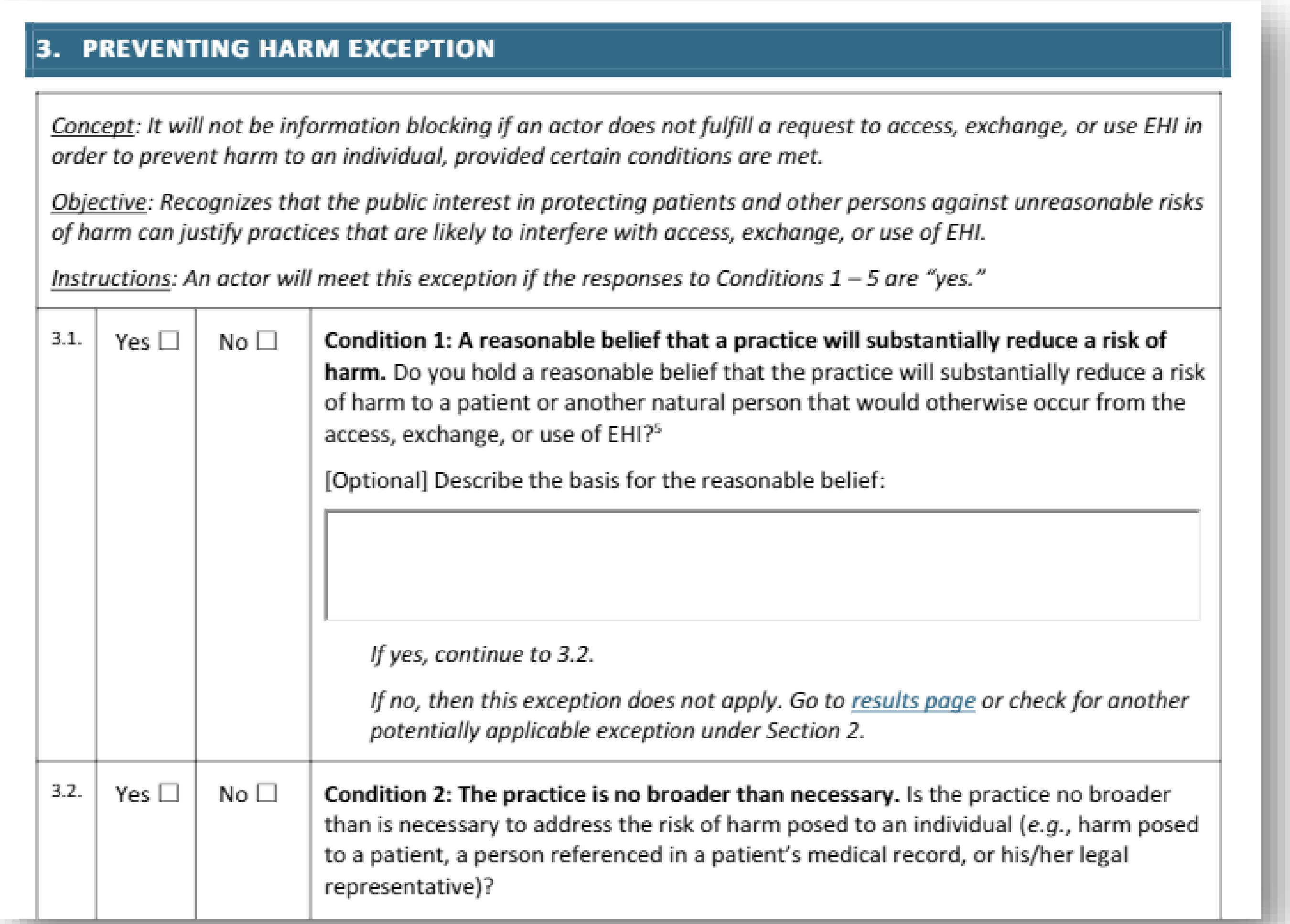


Name of System:	
Access, Exchange, or Use of EHI is: DENIED	
Examples: Denying a patient's request for EHI Denying a third party request that is accompanied by a patient's authorization Denying a researcher's request for EHI Denying a competitor's request for EHI Denying exchange of psychotherapy notes w/o patient consent	Exempt? Req. by Law Not EHI N/A
Access, Exchange, or Use of EHI is: DELAYED	
Examples: Delaying genetic testing results until clinician counsels patient Delaying release of imaging results until released by clinician	Exempt? Req. By Law Not EHI

DWT Information Blocking Toolkit, © 2020 Davis Wright Tremaine LLP

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?



3. PREVENTING HARM EXCEPTION

Concept: It will not be information blocking if an actor does not fulfill a request to access, exchange, or use EHI in order to prevent harm to an individual, provided certain conditions are met.

Objective: Recognizes that the public interest in protecting patients and other persons against unreasonable risks of harm can justify practices that are likely to interfere with access, exchange, or use of EHI.

Instructions: An actor will meet this exception if the responses to Conditions 1 – 5 are “yes.”

3.1.	Yes ☐	No ☐	**Condition 1: A reasonable belief that a practice will substantially reduce a risk of harm.** Do you hold a reasonable belief that the practice will substantially reduce a risk of harm to a patient or another natural person that would otherwise occur from the access, exchange, or use of EHI?[5] [Optional] Describe the basis for the reasonable belief: *If yes, continue to 3.2.* *If no, then this exception does not apply. Go to results page or check for another potentially applicable exception under Section 2.*
3.2.	Yes ☐	No ☐	**Condition 2: The practice is no broader than necessary.** Is the practice no broader than is necessary to address the risk of harm posed to an individual (*e.g.*, harm posed to a patient, a person referenced in a patient’s medical record, or his/her legal representative)?

DWT Information Blocking Toolkit, © 2020 Davis Wright Tremaine LLP

Takeaways

Takeaways

- November 2, 2020 will be here sooner than you think, start building information blocking program
  - Convene stakeholders
  - Identify information systems
  - Assess practices within those information systems
  - Check each practice against the Exemptions and 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.

Michaela B. Andrawis

Associate | Los Angeles

213.633.8649

michaelaandrawis@dwt.com

Michaela provides guidance to healthcare providers on regulatory matters such as Medicare and Medicaid coverage, reimbursement, Stark and anti-kickback laws, provider licensure requirements, health information privacy, financial relationships between providers, peer review and credentialing, and corporate and medical staff governance. She is experienced in counseling healthcare organizations regarding operational issues and regulatory compliance, and works with clients to provide practical and effective resolutions.