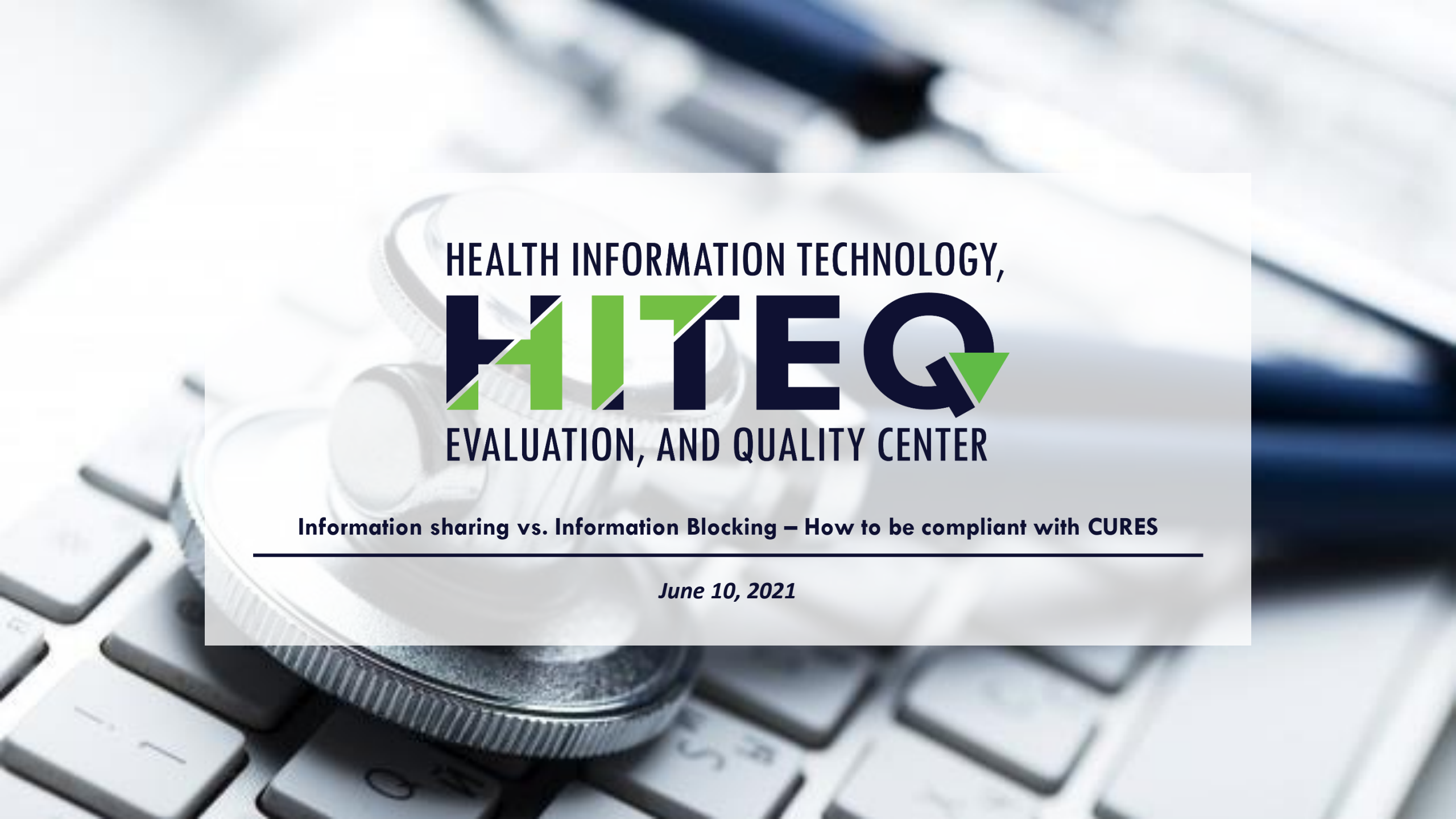


HEALTH INFORMATION TECHNOLOGY, HITEQ EVALUATION, AND QUALITY CENTER

Information sharing vs. Information Blocking – How to be compliant with CURES

June 10, 2021

COMMUNITY HEALTH CARE ASSOCIATION of New York State

The NYS-HCCN & The HITEQ Center Presents

Information Sharing vs. Information Blocking:

How to be Compliant with CURES

June 10, 2021

Intro to HITEQ

The HITEQ Center is a HRSA-funded National Training and Technical Assistance Partner (NTTAPs) that collaborates with HRSA partners including Health Center Controlled Networks, Primary Care Associations and other NTTAPs to engage health centers in the optimization of health IT to address key health center needs through:

- A **national website** with health center-focused resources, toolkits, training, and a calendar or related events.
- **Learning collaboratives, remote trainings,** and **on-demand technical assistance** on key content areas.

email us at hiteqinfo@jsi.com!

HITEQ Topic Areas

Access to comprehensive care using health IT and telehealth

Privacy and security

Advancing interoperability

Electronic patient engagement

Readiness for value based care

Using health IT and telehealth to improve Clinical quality and Health equity

Using health IT or telehealth to address emerging issues: behavioral health, HIV prevention, and emergency preparedness

The New York Statewide Health Center Controlled Network

Enhancing the patient & provider experience

Advancing interoperability

Using data to enhance value

Eric Pan, MD, MSc, FAMIA

- HITEQ lead for EHR and Interoperability
- Senior Physician Informaticist at Westat
- Trained in Internal Medicine and Informatics
- Decade-long experience leading HIE evaluation for VA's Veteran Health Information Exchange (VHIE, previously VLER) project
- Lead author of AHRQ's Guide to Evaluating Health Information Exchange Projects
- Coauthor of NAM's EHR ROI paper
- Member of AMIA's CURES NPRM response team

- EricPan@Westat.com

Today's Agenda

- Sharing Patient Information?
  - ONC's picture
  - HIPAA vs. CURES/Information Blocking
- How does ONC implement/interpret the CURES Act?
  - What is expected of health IT vendors?
  - What is expected of providers?
  - What are reasonable exceptions?
- How can health centers avoid information blocking
  - What need to be in place?
  - What are the key steps?

A lack of seamless data exchange in healthcare…

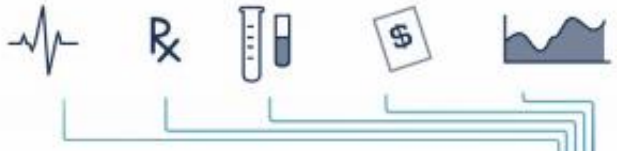
leads to disconnected care, worse health outcomes, and higher costs.

Interoperable healthcare data exchange…

enables coordinated care, improved health outcomes, and reduced cost.

How might these proposals impact me?

1. I can **easily access my health claims data**, including information about my treatment history and prescriptions.



2. I can easily find an **up-to-date list of providers** in my network.

3. I can **bring my data with me** when I switch plans or providers.

4. I know my coverage benefits are being **coordinated**.

5. I know which providers are sharing data, and **reports about data blocking** help me choose where to get care.

6. **Better communication** between my providers means I don't fall through the cracks.

The proposals would help empower me to take ownership over my health data.

A new EHI sharing paradigm

- HIPAA
  - Covered entities are permitted, but not required, to disclose ePHI in most circumstances
- CURES/Information Blocking
  - "Covered entities" (Health IT developers, providers, HIE) are required to provide access, exchange, or use of EHI unless prohibited by law or covered by one of the exceptions

Purpose of the CURES Act & ONC Final Rule

The Office of the National Coordinator for Health Information Technology

Purpose of the Final Rule

- ✓ **Patients**: Right of Access to their Chart, Supporting Patient Privacy and Security, the Ability to Shop for Care and Avoid Bankruptcy
- ✓ **Doctors and Hospitals**: Making Patient's Chart Data Requests Easy and Inexpensive, Allowing Choice of Software, Implementation
- ✓ **Patients, Doctors, and Hospitals**: Improving Patient Safety
- ✓ **Health IT Developers**: Minimizing API Development and Maintenance Costs, Protecting Intellectual Property
- ✓ **American Public**: Maximizing Innovation, Transparency in Health Care

§4002 – EHR certification

§4006 – Patient access

- HHS must
  - Encourage HIE & others to offer patient access to EHI
  - Educate providers on HIE
  - Offer best practice guidance to HIE
  - Facilitate electronic patient communication with providers
  - Assist patients & providers to understand a patient's right to access & protect PHI
- ONC must ensure patient access to health information in a convenient form

- ***Focused on Federal policies and patient rights rather than specific health IT requirements for providers (e.g., patient portal)***

§4004 – Information Blocking

- Defines “information blocking”
- Authorizes the Secretary to identify, through rulemaking, reasonable and necessary activities that do not constitute information blocking
- Identifies the HHS Office of Inspector General (OIG) as the HHS office to investigate claims of information blocking and provides referral processes to facilitate coordination with the HHS Office for Civil Rights (OCR)
- Prescribes up to $1M penalties for information blocking
- Charges ONC with implementing a complaint process for reporting information blocking, and provides confidentiality protections for complaints

Yes, there is an ONC information blocking complaint page

The Office of the National Coordinator for Health Information Technology

Help Us Stop Information Blocking

The Department of Health and Human Services is working to identify and stop instances of information blocking. You can help by reporting complaints about information blocking to us via http://www.healthIT.gov/healthITcomplaints.

What is information blocking? **Information blocking (or data blocking) occurs when individuals or entities — such as healthcare providers or IT vendors — knowingly and unreasonably interfere with the exchange or use of electronic health information.**[1] Information blocking is a serious problem because it can prevent timely access to information needed to manage patients' health conditions and coordinate their care. Further, it can prevent information from being used to improve health, make care more affordable, and research new treatments and cures.

Identifying information blocking: Information blocking can happen as a result of overt actions or policies that prevent electronic health information from being appropriately shared or used for authorized purposes. It can also occur in more subtle ways, such as through contract terms, organizational policies, or technical limitations that discourage or make it unnecessarily costly or burdensome to share and use information. Not all actions that impede the exchange or use of electronic health information constitute information blocking: sometimes the "blocking" may be necessary to protect patient safety, privacy, or other compelling interests.

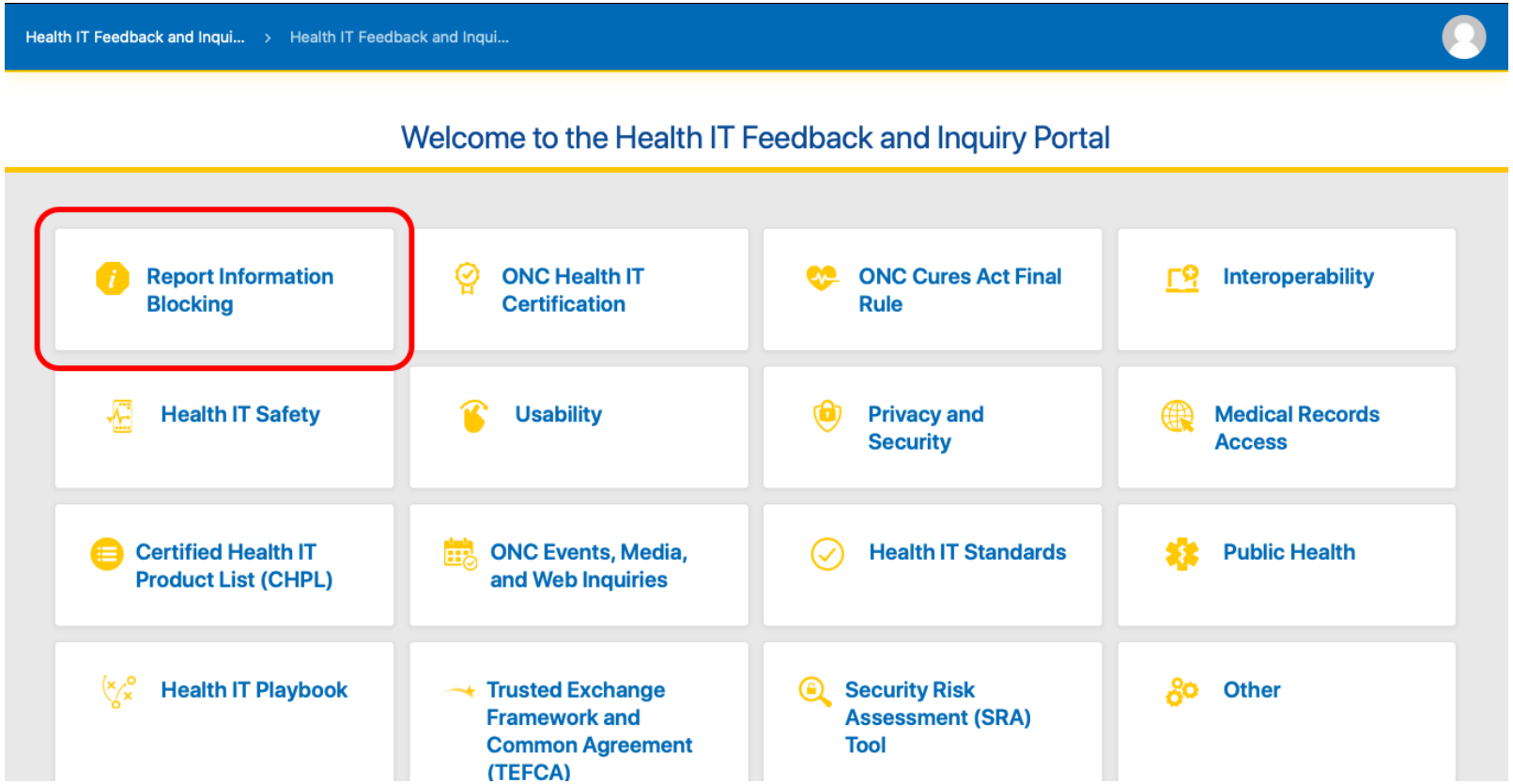
Some examples of conduct that may raise information blocking concerns include:

- Fees are imposed that make exchanging electronic health information cost prohibitive.
- An organization's policies or contractual arrangements prevent sharing or limit how information is shared with patients or their healthcare providers.
- The HIPAA Privacy Rule is inappropriately cited as a reason not to share information.
- Healthcare providers or IT vendors limit or discourage sharing information with other providers or with users of other IT systems.
- Technology is designed or implemented in non-standard ways that lessen the ability to exchange and use information with other IT systems, services, or applications that follow nationally recognized standards.
- Patients or healthcare providers become "locked in" to a particular technology or healthcare network because their electronic health information is not portable.

Help us stop information blocking and move toward nationwide interoperability by reporting information blocking via http://www.healthIT.gov/healthITcomplaints.

NOTICE: Depending on the nature of your complaint, we may contact you for additional information and, in some instances, may share the information you provide with other appropriate federal and state government agencies, officials, and authorities. Please note that while we will endeavor to keep the information you share with us confidential, federal or state laws may require us to disclose certain information in some circumstances. While legal and administrative constraints prevent us from responding to every complaint, all information is carefully reviewed and shared with appropriate officials. Your feedback is appreciated and helps us to improve our awareness and ability to address health IT-related issues and challenges.

[1] Office of the National Coordinator for Health Information Technology, *Report to Congress on Health Information Blocking* (April 2015), available at https://www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf.



Key Dates for Information Blocking

- Requirement for compliance – April 5, 2021

- First 24 months after final rule (October 6, 2022) – only need to share subset of EHI represented by US Core Data for Interoperability (USCDI) v1
  - USCDI & other standards to be discussed on Feb 10

- After first 24 months(after October 6, 2022) – all EHI

§4004 – Provider Information Blocking

- If a healthcare provider engages in the practice, it is only information blocking if the provider knows that such practice is unreasonable and is likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI.

§4004 – Health IT Information Blocking

- If a health IT developer*, exchange, or network engage in the practice, it is only information blocking if they know or should know that the practice is likely to interfere with, prevent, or materially discourage the access, exchange, or use of EHI.

- *"health IT developer" include distributor/reseller

Key Terms - Interfere

17

The Office of the National Coordinator for Health Information Technology

"Interfere with" or "Interference" What is it?

Interfere with or interference means to prevent, materially discourage, or otherwise inhibit.

- ***Publication of "FHIR service base URLs" (sometimes also referred to as "FHIR endpoints")*** – A FHIR service base URL 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.
- ***Delays*** – An actor's practice of slowing or delaying access, exchange, or use of EHI could constitute an interference and implicate the information blocking provision.
- ***Costs for Electronic Access by Patients/Individuals*** – An actor's practice of charging an individual, their personal representative, or another person or entity designated by the individual for electronic access to the individual's EHI would be inherently suspect under an information blocking review.

Provider actions that could be considered Information Blocking

- Limiting technology
  - Disabling the use of an EHR capability that would enable staff to share EHI with users at other systems
- Unreasonable delays
  - Taking several days to respond, despite having the capability to provide same-day EHI access in a format requested by patient or an unaffiliated provider

There are always exceptions!

Preventing Harm exception

- It will not be information blocking for an actor to engage in practices that are reasonable and necessary to prevent harm to a patient or another person, provided certain conditions are met.
- Required conditions
  - Reasonable belief that the action will substantially reduce a risk of harm to patient or another person
  - The action is no broader than necessary
- Examples
  - Decline to share data that is known to be inaccurate
  - Decline to share data from patient misidentification/mismatch
  - Refrain from disclosure that would endanger life/physical safety of a patient (must be determined by a provider with a clinician-patient relationship)

Privacy exception

- It will not be information blocking if an actor does not fulfill a request to access, exchange, or use EHI in order to protect an individual's privacy, provided certain conditions are met.
- Qualifying conditions
  - Legal requirement not satisfied;
  - Health IT developer not covered by HIPAA (e.g., consumer apps);
  - Denied under HIPAA privacy rule; or
  - Respecting an individual's request not to share information
- Examples
  - State/Federal requirements for patient consent
  - Information obtained from non-health care providers under the promise of confidentiality

Security exception

- It will not be information blocking for an actor to interfere with the access, exchange, or use of EHI in order to protect the security of EHI, provided certain conditions are met.
- Required conditions
  - Directly related to safeguarding the confidentiality, integrity, and availability of EHI;
  - Tailored to specific security risks; and
  - Implemented in a consistent and non-discriminatory manner.
- Document
  - Written organizational policies; or
  - Case-by-case determination showing that no reasonable alternatives to address the security risk that are less likely to interfere

Infeasibility exception

- It will not be information blocking if an actor does not fulfill a request to access, exchange, or use EHI due to the infeasibility of the request, provided certain conditions are met.
- Qualifying conditions
  - Uncontrollable events;
  - Inability to segment requested EHI from EHI that could not be shared per request, law, or Preventing Harm exception; or
  - Infeasible under the circumstances (documented at the time of request).
- **Written response must be provided within 10 business days**
- Examples
  - Natural disasters, public health emergency, loss of internet

Health IT performance exception

- It will not be information blocking for an actor to take reasonable and necessary measures to make health IT temporarily unavailable or to degrade the health IT's performance for the benefit of the overall performance of the health IT, provided certain conditions are met.
- Key conditions
  - Be implemented for a period of time no longer than necessary; and
  - Be implemented in a consistent and non-discriminatory manner
- Examples
  - EHR upgrade
  - Temporarily disable access to a 3rd party app that is negatively impacting the health IT performance (must be based on existing standard/service level agreement)

Content and manner exception

- It will not be information blocking for an actor to limit the content of its response to a request to access, exchange, or use EHI or the manner in which it fulfills a request to access, exchange, or use EHI, provided certain conditions are met.
- Content conditions
  - Only EHI identified by USCDI before Oct 6, 2022
- Manner conditions
  - Alterative manner to fulfil a require when technically unable to fulfill the request in any manner requested, or cannot reach agreeable terms with the requestor

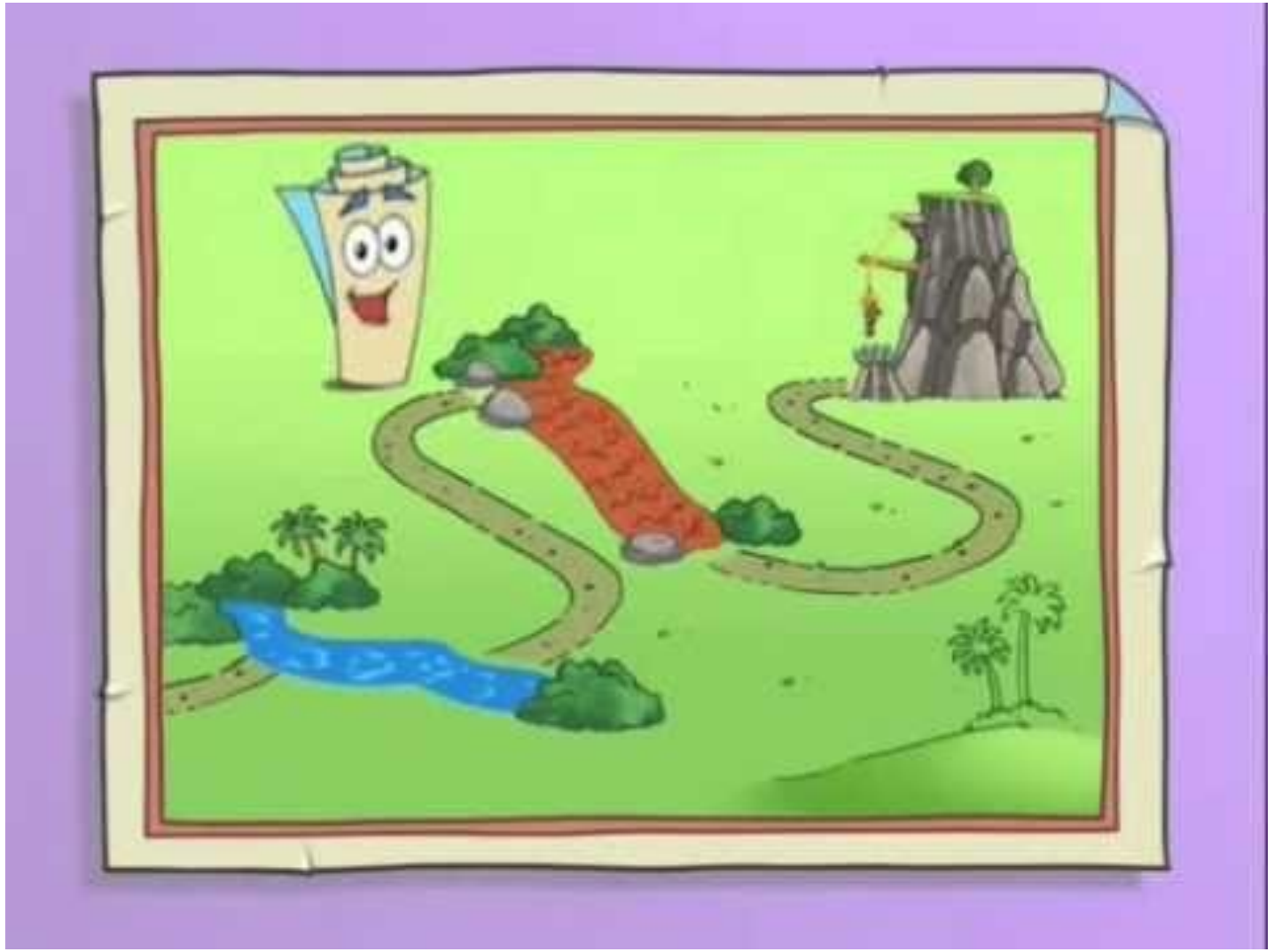
Fees exception

- It will not be information blocking for an actor to charge fees, including fees that result in a reasonable profit margin, for accessing, exchanging, or using EHI, provided certain conditions are met.
- Key conditions
  - Fee is based on objective and verifiable criteria that are uniformly applied
  - Fee is reasonably related to the provider's cost
  - Not affected by whether the requestor is a competitor

Licensing exception (vendor/HIE)

- It will not be information blocking for an actor to license interoperability elements for EHI to be accessed, exchanged, or used, provided certain conditions are met.
- Key conditions
  - Must begin license negotiations with the requestor within 10 business days
  - Negotiate a license within 30 days
  - Reasonable and on-discriminatory licensing terms
- Example
  - Applies to when health centers negotiate for hardware, software, integrated technologies, technical information, privileges, rights, IP, upgrades, or services that may be necessary to access, exchange, or use EHI

Pathway to compliance



Step 1 – Integrate with existing compliance efforts

- Review current structures, policies, procedures, and resources for compliance
  - HIPAA compliance
  - HRSA/BPHC funding & reporting compliance
- Subject matter experts
  - Legal counsel with health care expertise
  - IT expertise with understanding of your health IT implementation
  - Information privacy experts

Step 1 – Integrate with existing compliance efforts

- Does your health center have consistent policies and procedures in place to respond to information request from patients and providers?

Step 2 – review existing policy

- How does your health center respond to request for access, exchange, or use of patient medical information?
  - HIPAA consideration
  - Local legal requirements
  - Confidentiality policy
  - Adolescent health and other sensitive health issues

Step 2 – review existing policy

- Have you made your office notes, lab results, and other diagnostic reports available to patients as soon as the health center receives an electronic copy?
  - Have you defined the difference between preliminary reports and final reports, and when they are incorporated into the official medical records?

Step 2 – review existing policy

- Have you removed any general delays (e.g., results are not released until provider review) in the release of your electronic health information (EHI) to patients?
  - Have you established procedures on how specific delays could be applied to specific patient-result combinations by providers who have cared for the patient?

Step 3 – Define exceptions

- Review each information blocking exception
- Address how each of the exceptions would be used in your health center
  - Detail all the requirements in your context
  - Applied as narrowly as possible
  - Applied in a non-discriminatory manner
- Note the limitation of your health IT
  - Data segmentation
  - Allowing individualized management of information release

Step 3 – Define exceptions

- Have you defined how your staff could identify sensitive information (e.g., behavioral health, HIV,…) in the medical records?
  - Have you defined how your health IT could segment them from other information in the medical records?

Step 4 – Define “Reasonableness”

- Provider Information Blocking requires knowing that the practice is “unreasonable” and likely to interfere with, prevent, or discourage access, exchange, or use of EHI
- Several exceptions require “reasonable” effort
- Define the level of effort reasonable to fulfill a request
- Define how a group of provider & staff can come together and establish a “reasonable” concern for patient harm
- Procedures need to be established for a detailed workflow where a case-by-case finding will be documented

Resources

- HITEQ Center HIE & Interoperability Resources
  - https://hiteqcenter.org/Resources/HIE-Interoperability
- Health IT Playbook
  - https://www.healthit.gov/playbook/
- CHIME Information Blocking cheat sheet
  - https://chimecentral.org/wp-content/uploads/2020/06/061420_CHIME-Information-Blocking-Cheat-Sheet-FINAL-RULE1-1.pdf
- AMA Information Blocking guides
  - https://www.ama-assn.org/system/files/2021-01/information-blocking-part-1.pdf
  - https://www.ama-assn.org/system/files/2020-11/info-blocking-compliance.pdf
- Information Blocking Resource center
  - https://infoblockingcenter.org/

Thank you for joining us today!

Connect with us | hccn@chcanys.org

This programming is supported by the Health Resources and Services Administration (HRSA) of the U.S. Department of Health and Human Services (HHS) as part of an award to CHCANYS' New York State Health Center Controlled Network (NYS-HCCN) totaling $3,666,000 with 0% financed with non-governmental sources. The contents are those of the author(s) and do not necessarily represent the official views of, nor an endorsement, by HRSA, HHS, or the U.S. Government. For more information, please visit HRSA.gov.