Preparing for Cures Act Regulatory Compliance, Part 1

Denise Webb, **MA, CPHIMS,** Health IT Executive Advisor, Pivot Point Consulting
Nick Loftin, MBA, Director, Virtual Care, Pivot Point Consulting

February 16, 2022

Disclaimers

- This presentation is for informational purposes only
- It does NOT, and is not intended to, constitute legal advice
- Only your attorney can provide assurances regarding the application of this information to your particular circumstances
- The statements, views and opinions expressed in this presentation are solely those of the presenter, and not those of CHCANYS
- The statements, views and opinions expressed in this presentation are solely those of the presenter, and not those of the ONC

Thank you for joining us today.
This is intended to teach and provide you with the information to have an informed discussion regarding how to address and meet the requirements of the information blocking provision and exceptions in your organization.

About the Empowering Patients Educational Series

- Designed to support CHCANYS members as they work toward compliance with information blocking regulations stemming from the 21st Century Cures Act
- November 2021-March 2022
- Includes:
  - Webinar presentations providing foundational knowledge for all member roles (provider, compliance, HIM)
  - Ask the Experts interactive Q&A sessions focusing on information needs of specific member roles
  - Supporting resources to help members operationalize the regulations within their organizations

Note that we've included a calendar slide at the end
Not only roles but use cases as well
Will be providing the recording and slides after the presentation

Agenda

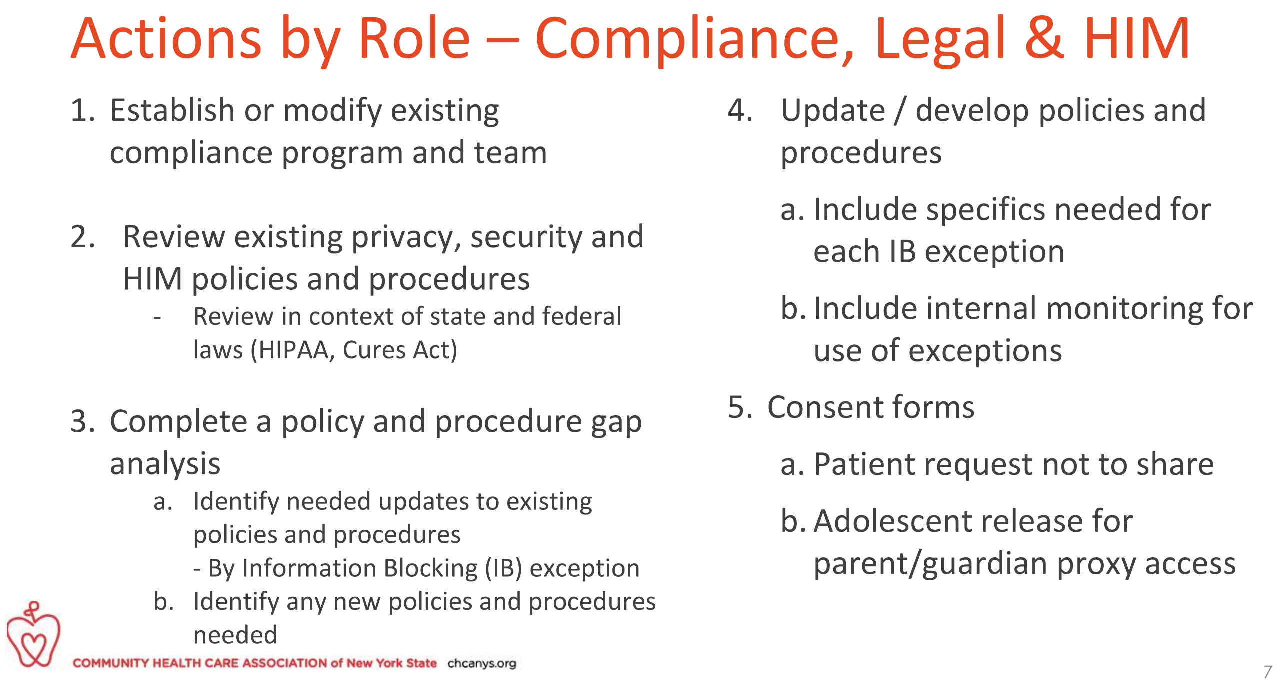
- Learning Objectives
- Who Needs to Take Action
- Actions by Role
- Next Steps
- Q&A

Today's Learning Objectives

- Understanding how your health center is affected by the ONC Cures Act Final Rule information blocking provision requirements from a health care policy and technology perspective
- Determining the subject matter experts and key activities needed to assist your health center in complying with the new information blocking regulations
- Recognizing how the requirements impact your health center's policies, procedures, workflows, and technology for sharing electronic health information (EHI) and fulfilling requests for legally permissible access, exchange, or use of EHI
- Facilitating and sustaining your compliance program and organizational change relevant to sharing EHI

Who Needs to Take Action?

- Entire health center must be involved and consistent, with leadership by and subject matter expertise from the following:
  - Compliance, Legal, including the Privacy Officer, and HIM
  - IT Department, including the Information Security Officer
  - Clinical Operations
  - Training and Marketing



Actions by Role – Compliance, Legal & HIM

1. Establish or modify existing compliance program and team
2. Review existing privacy, security and HIM policies and procedures
   - Review in context of state and federal laws (HIPAA, Cures Act)
3. Complete a policy and procedure gap analysis
   a. Identify needed updates to existing policies and procedures
      - By Information Blocking (IB) exception
   b. Identify any new policies and procedures needed
4. Update / develop policies and procedures
   a. Include specifics needed for each IB exception
   b. Include internal monitoring for use of exceptions
5. Consent forms
   a. Patient request not to share
   b. Adolescent release for parent/guardian proxy access

COMMUNITY HEALTH CARE ASSOCIATION of New York State chcanys.org

Compliance program and team

Do you have an existing compliance program and team in place to monitor and take action on compliance/ privacy

Understand that ppl have multiple roles

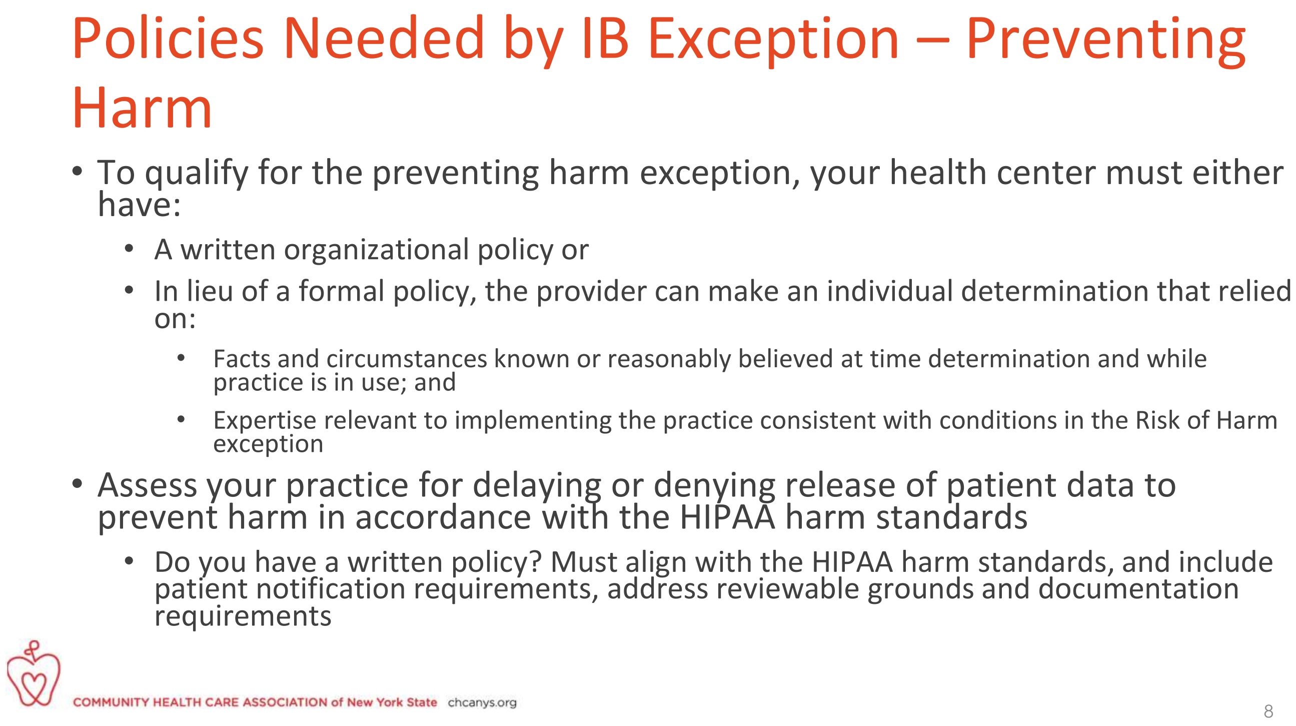
Do you have an existing compliance program?

If yes, then you can start with your existing structure, policies, procedures, and resources as a foundation for compliance with the information blocking regulation. The regulations and requirements are probably going to be new to most people in your organization and your compliance staff may have limited knowledge about the information blocking provision and exceptions to sharing EHI.

If you don’t have a compliance program, you should create one for compliance with both HIPAA and information blocking regulations and establish a compliance team.

To review and modify your existing compliance program or to create a new program, you will need to involve your subject matter experts, such as your legal counsel to interpret and advise on the regulations and laws, your IT staff and information security officer to understand how your organization handles access, exchange, and use of EHI now and what needs to be changed, and your privacy officer and HIM staff who understand how your organization protects the privacy of PHI and complies with federal and state privacy laws, such as HIPAA, and how requests for records and records release is handled now by your organization.

Policies and procedure review, gap analysis, and development help to identify what changes are needed by understanding current state, while informing future state and training needs



Policies Needed by IB Exception – Preventing Harm

- To qualify for the preventing harm exception, your health center must either have:
  - A written organizational policy or
  - In lieu of a formal policy, the provider can make an individual determination that relied on:
    - Facts and circumstances known or reasonably believed at time determination and while practice is in use; and
    - Expertise relevant to implementing the practice consistent with conditions in the Risk of Harm exception
- Assess your practice for delaying or denying release of patient data to prevent harm in accordance with the HIPAA harm standards
  - Do you have a written policy? Must align with the HIPAA harm standards, and include patient notification requirements, address reviewable grounds and documentation requirements

Before talking about the policies needed specifically for the information blocking exceptions, I want to say a few things about policy development in general. Your written policies should be cover what must be done and by whom—roles and responsibilities for implementing the policy. Oftentimes, I see organizations include process and procedures in their policy documents, and these are difficult to maintain. Your processes and procedures answer how a policy is implemented. Typically, a policy has a longer life than a process or procedure and usually only needs to be changed to respond to changes in laws or regulations. Procedures and processes on the other hand continually evolve and change, especially as technology or business practices change. My advice to you, is keep your policies short and to the point on what everyone is required to do and point to the procedures/processes on how to implement the policy. Since both HIPAA and the Cures Act generally focus on privacy, security, and the management of health information, you may want to consider putting all the relevant policies into a combined policy manual. Your team will need to review existing business associate agreements and contracts to ensure there is not any language in these that may result in interfering with legally permissible access, exchange, or use of EHI and modify the language if necessary.

Just to remind everyone, of the eight IB exceptions, five address practices that delay or deny fulfilling requests for access, exchange, or use of EHI and the remaining three address how the requests have to be fulfilled for legally permissible requests for EHI. I will be addressing policies and procedures needed for seven of the eight exceptions., excluding the licensing exception as that exception doesn't typically apply to provider organizations, unless your health center develops and licenses certified health IT. The first three exceptions: "Preventing Harm," "Privacy," and "Security" are structured to operate in a manner consistent with the HIPAA Privacy and Security rules, so your Center should not require significant changes to existing HIPAA policies and will more likely need to make changes to existing processes, procedures, and documentation.

The compliance team should start with a review of its HIPAA policies and procedures.
To qualify for the preventing harm exception, your health center must either have:
A written organizational policy or
In lieu of a formal policy, your providers can make an individual determination based on facts and circumstances and expertise.

I will cover some of the questions your compliance team should answer in completing their review and assessment of your current policy, assuming you have one. If not, these questions will inform you on what is needed in your policy. All of this information will be included in a compliance checklist we will provide you in March.

Do you have a written policy?

How do your providers currently determine that withholding certain health information from a patient or the patient's representative will substantially reduce the risk of harm to the patient or another person referenced in the health information? Note that access to the health information must be reasonably likely to cause substantial harm which includes harm to life or physical safety and does not include emotional harm.

What are your health center's current documentation requirements for these determinations? ONC's rule does not require specific or unique documentation for risk of harm determinations by the health care professional. We as well as ONC suggest documenting these determination in the EHR would be considered an appropriate approach.

How does your policy address risk of harm due to data integrity issues? Consider what your current process is, if any, for addressing data integrity issues with your IT Department or vendor supporting your systems

Does your policy require denials be written in plain language and describe the basis for denial?

Does the policy require that denials describe the individual's right to have the decision reviewed, how to request this review, and how to submit a complaint to the health center or HHS OCR?

Do you notify individuals in writing within 30 days (or 60 days if you notified individual of an extension) of the denial?

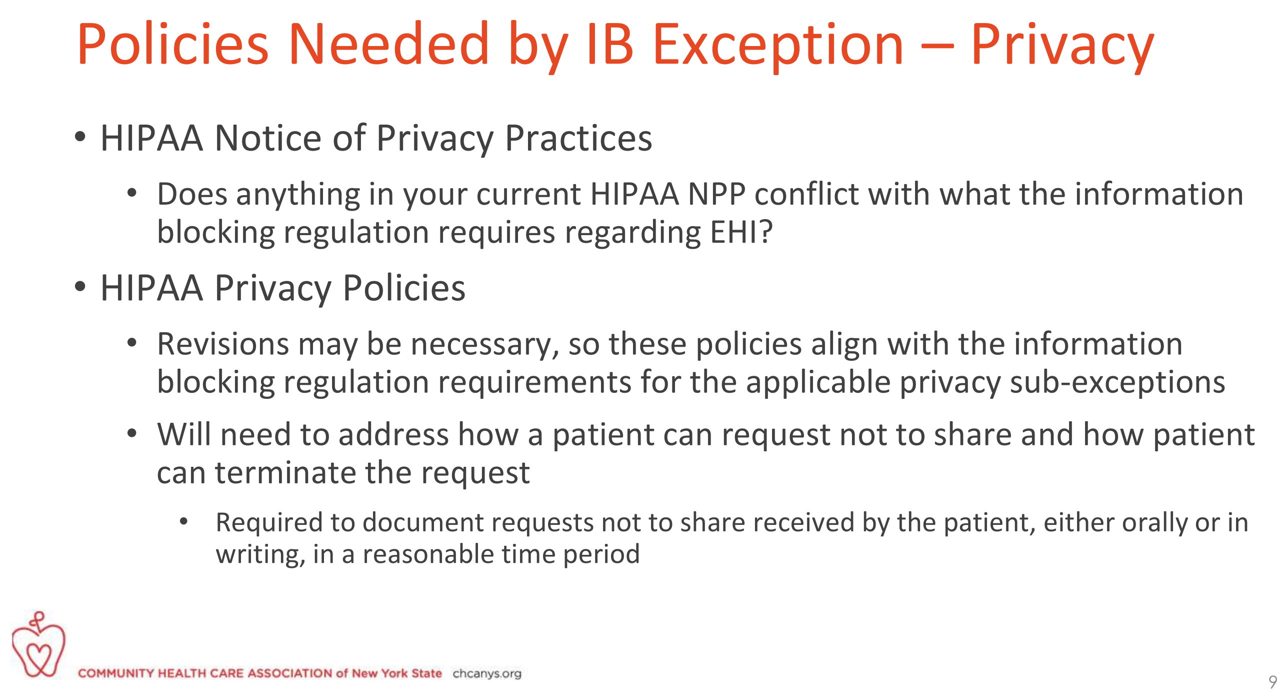
Does the policy address denials that have reviewable grounds and include a designated reviewing official?

Does the reviewing official have a set period of time to reaffirm or reverse a denial?

Does the policy require prompt written notification to the individual on the reviewing official's determination as well as other actions required to carry out the determination?

The organizational policy should require that each practice of denying access to EHI to reduce risk of harm conforms to the conditions in the Preventing Harm exception:

- ✓ Reasonable belief the practice will substantially reduce risk of harm
- ✓ Breadth of practice is no broader than necessary
- ✓ Meets at least one condition from the "Type of Risk" and "Type of Harm" categories in the Preventing Harm exception
- ✓ Providers implement the practice in a consistent and non-discriminatory manner
- ✓ Accounts for a patient's review rights (when applicable) and reversal of provider's determination to deny or delay access to patient's EHI



Policies Needed by IB Exception – Privacy

- HIPAA Notice of Privacy Practices
  - Does anything in your current HIPAA NPP conflict with what the information blocking regulation requires regarding EHI?
- HIPAA Privacy Policies
  - Revisions may be necessary, so these policies align with the information blocking regulation requirements for the applicable privacy sub-exceptions
  - Will need to address how a patient can request not to share and how patient can terminate the request
    - Required to document requests not to share received by the patient, either orally or in writing, in a reasonable time period

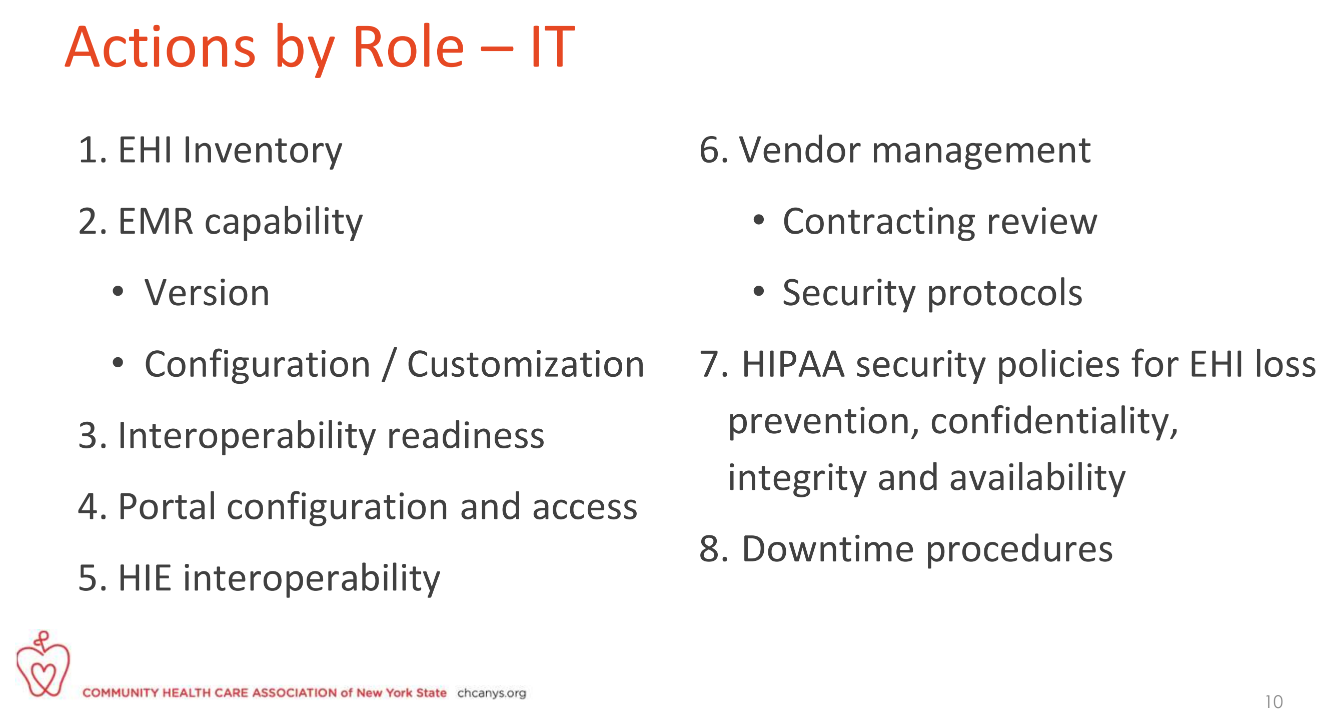
Your compliance team should review your existing HIPAA Notice of Privacy Practices (HIPAA NPP).

Does anything in your current HIPAA NPP conflict with what the information blocking regulation requires regarding EHI under the Privacy Exception? Three of the four sub-exceptions will apply to provider organizations: pre-condition not being satisfied to fulfill a request for EHI denying a request to be consistent with the HIPAA privacy rule, and if patient requests not to share his or her EHI.

In your HIPAA policies, review your current requirements in your medical records policies dealing with access to patient data. Revisions may be necessary so these policies align with the information blocking regulation requirements and in addition to these revisions, your health center may want to have specific provisions in an existing privacy policy or a separate policy that addresses the conditions of the information blocking privacy exception. For easier maintenance, we suggest you address the policy, practice, and procedural requirements of each information blocking exception in your existing policy, practice, and procedural documentation or create the documentation if it doesn't already exist.

For any practice that doesn't conform with your organizations policies and procedures, your organization will have to document on a case-by-case basis how it reached its decision to not fulfill a request for EHI for privacy reasons, including any privacy pre-condition criteria that were not met and why, in the case where a pre-condition to share a patient’s data was not met and you denied access to the EHI.

Procedurally, how will you or do you presently handle denial of requests to comply with HIPAA or requests from patients not to share data? Do you respond to these requests in a reasonable amount of time?



Actions by Role – IT

1. EHI Inventory
2. EMR capability
   - Version
   - Configuration / Customization
3. Interoperability readiness
4. Portal configuration and access
5. HIE interoperability
6. Vendor management
   - Contracting review
   - Security protocols
7. HIPAA security policies for EHI loss prevention, confidentiality, integrity and availability
8. Downtime procedures

COMMUNITY HEALTH CARE ASSOCIATION of New York State chcanys.org

EHI Inventory- in conjunction with Ops

While much of a patient's EHI may be within the EHR, the health center should identify any EHI that is not available in the EHR and resides in other systems, such as the Practice Management, Revenue Cycle Management systems or PACs. The definition of EHI reverts to the full scope of ePHI data in the designated record set, not just the data elements represented in the USCDI standard, on of October 6, 2022.

Need a definition of the legal medical record (helps with EHI inventory)

EMR capability

1. Version
   1. What is needed to get your EMR to compliance
      1. Multi-version upgrades
      2. Is EMR SaaS or internally managed?

2. Configuration and customization

    1. What can your center do to maximize electronic health information sharing workflows?

Interoperability readiness –is your IT department or your EHR vendor hosting and managing your FHIR server and endpoints and app registration?

1. HL7

2. Smart on FHIR

3. USCDI & TEFCA

Portal configuration and access

a. Auto-sharing / delivery of patient records – will need to address any set timeframes in policies or procedures that will delay delivery of test results once available

b. Proxy access--segment data for teens/adolescents and parents

HIE Interoperability – are you participating in an HIE? If not, consider what your organization's response will be to patient requests for their EHI to be sent to the HIE

Vendor management

a. Contracting review

    i. Licensing agreement

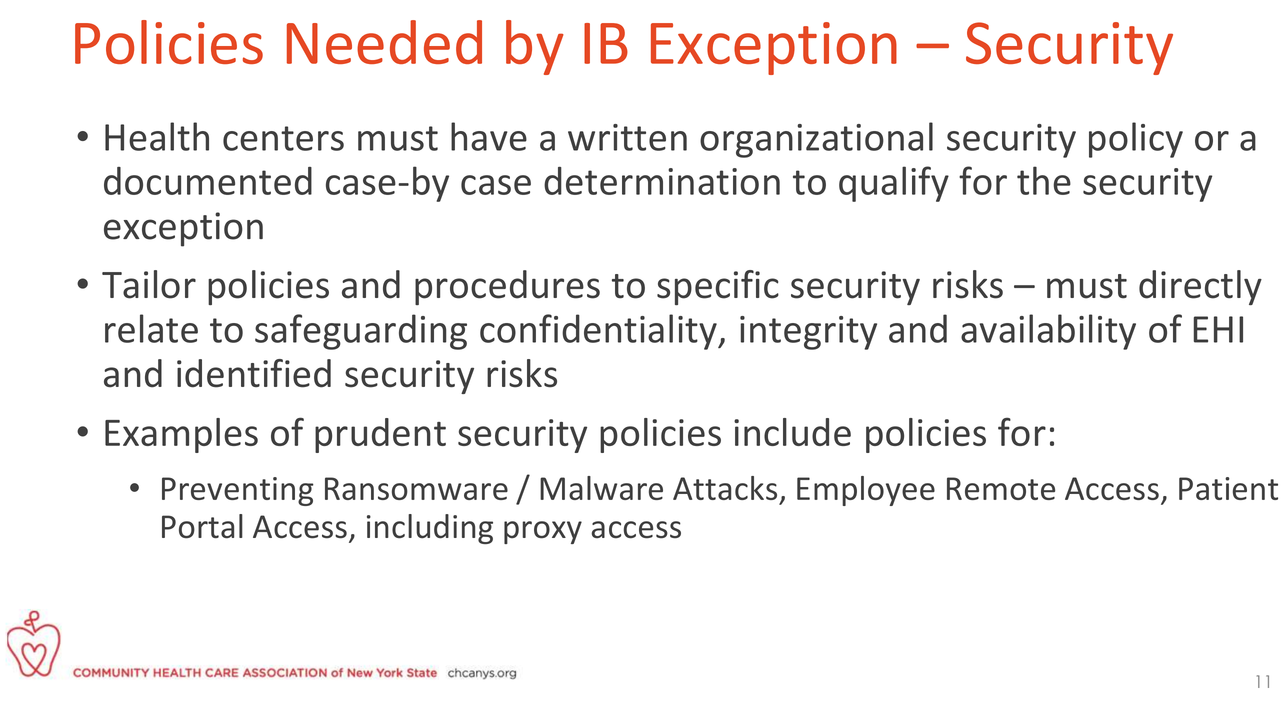
    ii. BAA/EULA/NDA

    iii. Downtime SLAs

    i. Internal need for emergency and planned downtime communication

b. Security protocols

Contract review: license must provide all rights necessary to: (1) enable the access, exchange, or use of EHI; and (2) achieve the intended access, exchange, or use of EHI via the interoperability elements



Policies Needed by IB Exception – Security

- Health centers must have a written organizational security policy or a documented case-by case determination to qualify for the security exception
- Tailor policies and procedures to specific security risks – must directly relate to safeguarding confidentiality, integrity and availability of EHI and identified security risks
- Examples of prudent security policies include policies for:
  - Preventing Ransomware / Malware Attacks, Employee Remote Access, Patient Portal Access, including proxy access

The Security exception addresses reasonable and necessary practices to protect the security of EHI that are likely to interfere with EHI access, exchange, or use but will not be considered information blocking if certain conditions are met. Your health center's security policies should be based on the security risks identified in your HIPAA Security Risk Assessment. For example, your policy for patient portal access may require a minimum amount of time to process a request for access and provision the portal account.

The **fourth condition** in the Security Exception requires a provider's practices that are likely to interfere with the access, exchange, or use of EHI be implemented in accordance with a written organizational security policy. The policy must:

1) Be based on and be directly responsive to security risks identified and assessed by or on behalf of your Center; align with one of more applicable consensus-based standards or best practice guidance; and
2) Provide objective timeframes and other parameters for identifying, responding to, and addressing security incidents.

In the case where your Center's security practice is not implementing a written organizational policy, the provider must have made a determination in each case based on the particular facts and circumstances that:

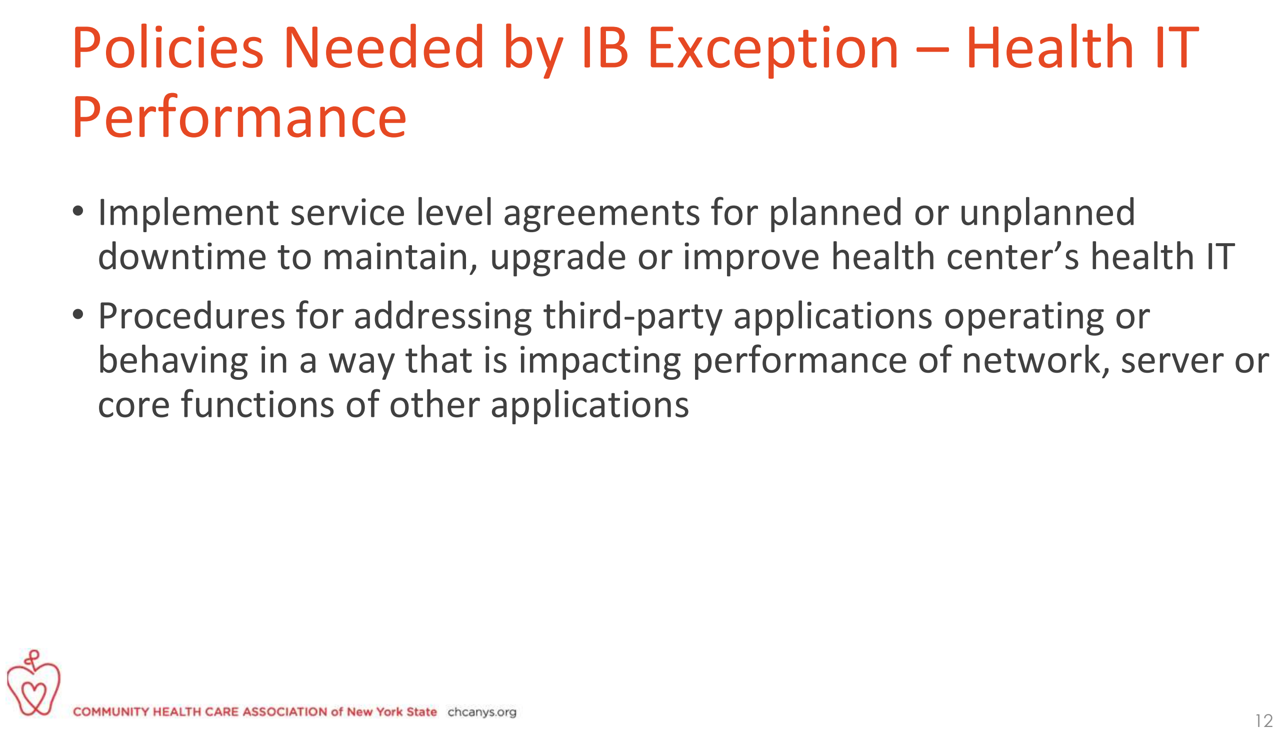
1) The practice is necessary to mitigate the security risk to EHI; and

2) There are no reasonable alternatives to the practice that address the security risk that are less likely to interfere with access, exchange, or use of EHI.
These case-by-case determinations should be documented.

The **first condition** under this exception is that the practice must be directly related to safeguarding the confidentiality, integrity, and availability of EHI. Substantiation of this condition being met by the provider includes but is not limited to the provider’s basis for adopting a particular security practice evidenced by the provider’s written organizational security policy, risk assessments the provider has performed that informed their security-based practice or practices, and other relevant documentation the provider maintains, such as documentation maintained as a part of its HIPAA security risk assessment and mitigation plans that supports meeting the HIPAA Security Rule.

The **second condition** is that the practice must be tailored to the specific security risk addressed. This condition presumes the provider evaluated the risks posed by the security threat and developed a response tailored to mitigate the health IT or other related system vulnerabilities.

The **third condition** is that the practice must be implemented in a consistent and non-discriminatory manner. This means the provider treats similarly situated actors whose interactions pose the same level of security risk consistently with one another under the provider’s security policies.



Policies Needed by IB Exception – Health IT Performance

- Implement service level agreements for planned or unplanned downtime to maintain, upgrade or improve health center’s health IT
- Procedures for addressing third-party applications operating or behaving in a way that is impacting performance of network, server or core functions of other applications

For the Health IT Performance exception, your Center will need to implement service level agreements for planned or unplanned downtime to maintain, upgrade, or improve health center’s health IT, either with your internal IT department or your managed services and EHR SaaS vendors. This also includes having written downtime procedures that your IT staff are trained on and follow. If you don’t have your own IT staff and you use a manage service provider, include this requirement in the service provider’s contract. These procedures should include a communication plan to inform end users, including patients.

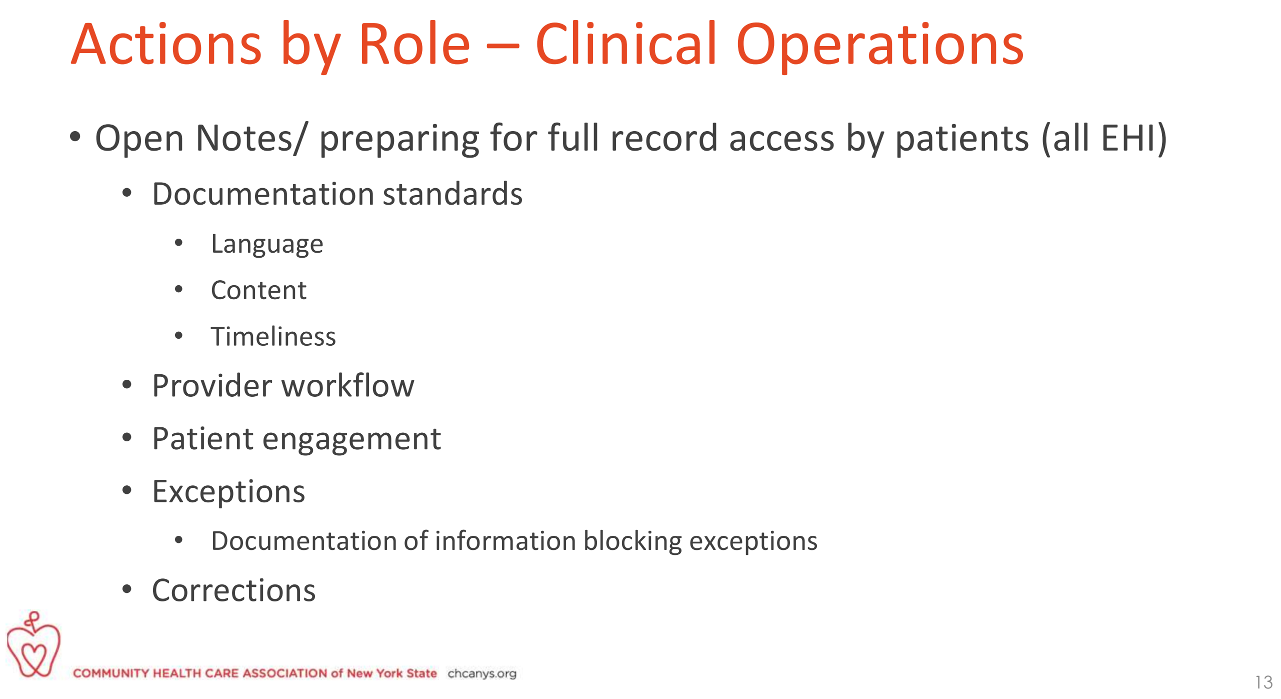
Downtime must be:

Implemented no longer than necessary
Implemented in a consistent and non-discriminatory way
Consistent with SLAs

Any health IT maintenance and improvements aimed at preventing harm to a patient or other person (in the case of data integrity issues that present a risk of harm) or to prevent a security risk need to comply with the Preventing Harm or Security exceptions, respectively.

For example, if an individual or application is making or attempting unauthorized access to systems or EHI, the entity with control of the system subject to the security risk should take prompt action to address the risk which might include health IT downtime or degradation. This would be covered under the Security exception and policies. An example is shutting down network access to stop a denial of service or malware attack.

Your Center will need procedures for addressing third-party applications operating or behaving in a way that is impacting performance of network, server or core functions of other applications. Dealing with an errant application may interfere with access, exchange, and use of EHI, but this will be OK if you have written procedures and deal with the errant application in a timely matter to restore service.



Actions by Role – Clinical Operations

- Open Notes/ preparing for full record access by patients (all EHI)
  - Documentation standards
    - Language
    - Content
    - Timeliness
  - Provider workflow
  - Patient engagement
  - Exceptions
    - Documentation of information blocking exceptions
  - Corrections

Patients may misread or misinterpret / misunderstand provider notes in their EHI. Providers will need to be vigilant and proactive in ensuring patients' records are accurate and informative and do not include terms or language that is offensive to the patient (avoiding use of sensitive words, such as "obese," "addict," "non-compliant," "non-cooperative," "patient refuses," etc.) Of course, providers should document difficult issues, but do it in a way that is non-offensive, yet accurately documents the issue. Providers should assume that all notes will be read by the patient and should recognize the practical and legal implications of this.

As in the past, providers will need to be careful when using templates, copy and paste, and the carry-forward features of the EHR. The accuracy and completeness of the information will be amplified with greater patient access to their EHI.

Internal questions

How long does it take to process and release records to patient?

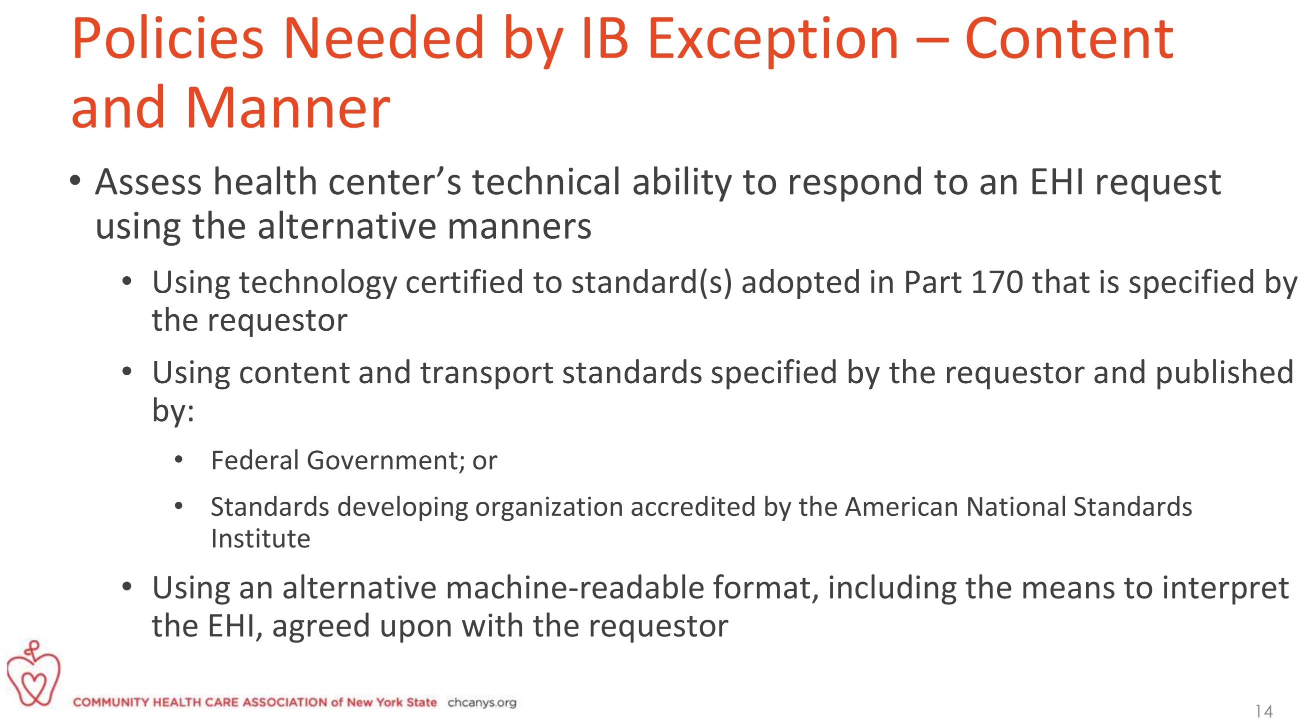
Re: delay for review of test results

(workflow) Build in templates/forms on documenting use of exceptions for use and denial of records

help from IT and/or vendor

Will touch on more by next time

Question to ask vendor: what do you have for documenting the use of exceptions….

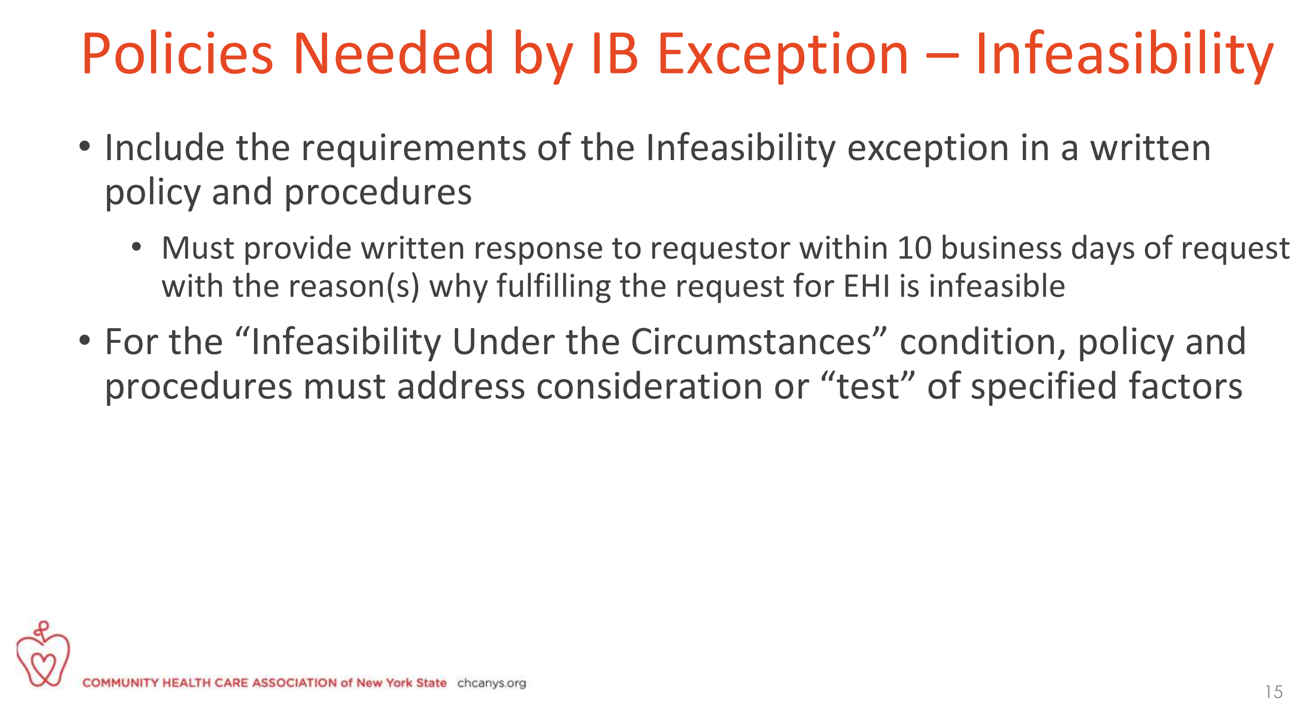


Policies Needed by IB Exception – Content and Manner

- Assess health center’s technical ability to respond to an EHI request using the alternative manners
  - Using technology certified to standard(s) adopted in Part 170 that is specified by the requestor
  - Using content and transport standards specified by the requestor and published by:
    - Federal Government; or
    - Standards developing organization accredited by the American National Standards Institute
  - Using an alternative machine-readable format, including the means to interpret the EHI, agreed upon with the requestor

Content and Manner Exception
Providers must meet BOTH conditions:
Content condition
Before October 6, 2022, EHI identified by the data elements represented in USCDI standard.
On and after October 6, 2022, EHI without the limitation.
AND
Manner condition
Any manner unless: (1) technically unable to fulfill in the manner requested; or (2) cannot reach agreeable terms with the requestor
If your health center responds in an alternative manner, the Center must fulfill the request without unnecessary delay in the following order of priority, only proceeding to the next consecutive alternative if technically unable to fulfill the request in the previous manner. Your Center will need to work with IT, HIM, and your clinical operations teams to develop processes and procedures for responding for EHI requests in any manner or one of the alternative manners and document the results, particularly if you determine it is infeasible under the circumstances to fulfill the request at all.

Note that your organization must comply with the fees requirements in HIPAA for fulling EHI requests using any of the alternative manners and that no fee may be charged to patients or their designees for electronic access as defined under the Fees Exception. Review your policies regarding charging fees for records access and ensure they comply and align with the Fees Exception.



Policies Needed by IB Exception – Infeasibility

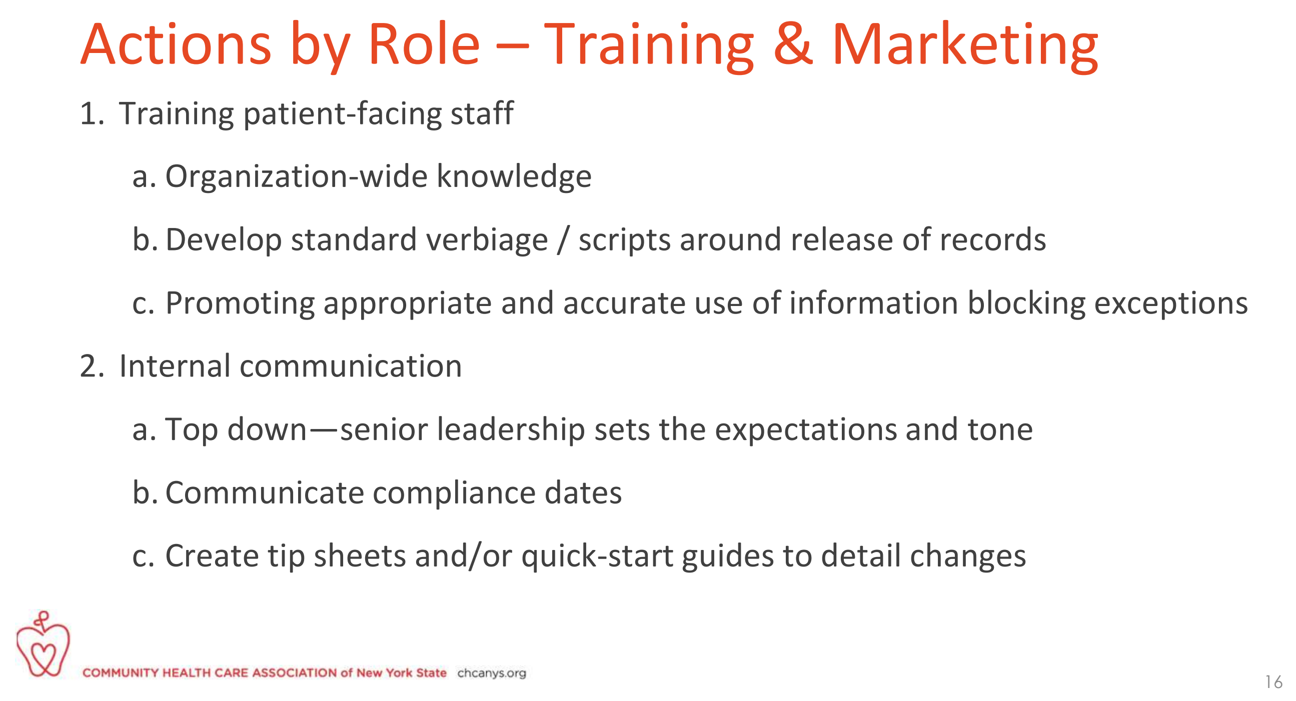
- Include the requirements of the Infeasibility exception in a written policy and procedures
  - Must provide written response to requestor within 10 business days of request with the reason(s) why fulfilling the request for EHI is infeasible
- For the "Infeasibility Under the Circumstances" condition, policy and procedures must address consideration or "test" of specified factors

For the Infeasibility exception, your Center must demonstrate that the practice meets 1 of 3 conditions:
Uncontrollable events beyond your control, OR
Segmentation which is when you cannot unambiguously segment the requested EHI from other EHI in your EHR or in your patient portal, OR
Infeasibility under the circumstances

Your Center must provide written response within 10 business days of request with the reason(s) why fulfilling the request for EHI is infeasible

Infeasibility Under the Circumstances – Factor Test

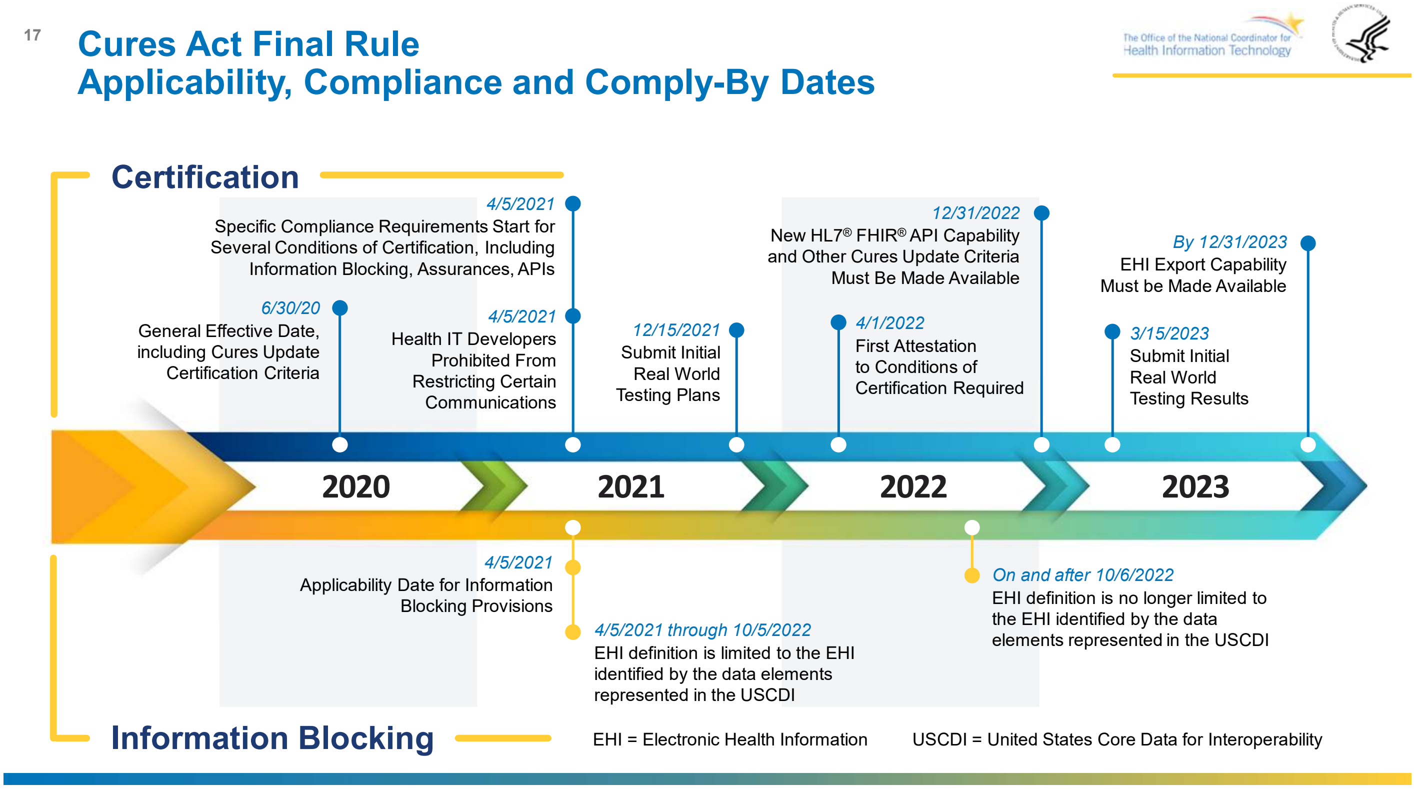
"…[T]hrough a contemporaneous written record or other documentation, provider's policy and procedure must give consistent and non-discriminatory consideration of the following factors…:"
Type of EHI and the purposes for which it may be needed;
Cost to your organization of complying with the request in the manner requested;
Financial and technical resources available to your organization;
Whether the practice is non-discriminatory and "same access comparison;"
Whether your organization owns or has control over the technology, platform, or HIN/HIE that holds the EHI; and
Why the Content and Manner Exception didn't "work" for the particular request



Actions by Role – Training & Marketing

1. Training patient-facing staff
   a. Organization-wide knowledge
   b. Develop standard verbiage / scripts around release of records
   c. Promoting appropriate and accurate use of information blocking exceptions
2. Internal communication
   a. Top down—senior leadership sets the expectations and tone
   b. Communicate compliance dates
   c. Create tip sheets and/or quick-start guides to detail changes

1. Training patient facing staff
   a. Organization-wide knowledge sharing
   b. Verbiage around release of records
   c. Accurate usage of exceptions
2. Internal communication
   a. Top down
      i. Change management
   b. Communicate compliance dates
   c. Create tip sheets and/or quick start guides to detail changes
3. Patient education
   a. Encourage portal utilization
   b. Inform of any changes in record access
   c. Inform how to file for amendments/ updates to their record



17

Cures Act Final Rule
Applicability, Compliance and Comply-By Dates

The Office of the National Coordinator for Health Information Technology

Certification

6/30/20
General Effective Date, including Cures Update Certification Criteria

4/5/2021
Specific Compliance Requirements Start for Several Conditions of Certification, Including Information Blocking, Assurances, APIs

4/5/2021
Health IT Developers Prohibited From Restricting Certain Communications

12/15/2021
Submit Initial Real World Testing Plans

4/1/2022
First Attestation to Conditions of Certification Required

12/31/2022
New HL7® FHIR® API Capability and Other Cures Update Criteria Must Be Made Available

3/15/2023
Submit Initial Real World Testing Results

By 12/31/2023
EHI Export Capability Must be Made Available

4/5/2021
Applicability Date for Information Blocking Provisions

4/5/2021 through 10/5/2022
EHI definition is limited to the EHI identified by the data elements represented in the USCDI

On and after 10/6/2022
EHI definition is no longer limited to the EHI identified by the data elements represented in the USCDI

Information Blocking

EHI = Electronic Health Information

USCDI = United States Core Data for Interoperability

Key dates:

4/5/21: Information Blocking provisions applicability date (complaints and enforcement can go back to this date)

10/6/22: Expanded definition of EHI to all ePHI in designated record set (beyond data elements represented in USCDI)

12/31/22: Your health IT vendor must make the EHR Cures updates available to you for USCDI (replaces CCDS in the interoperability certification criteria) and the FHIR R4 Patient and

Population API

12/31/23: EHI export capability must be made available to healthcare organizations

Key Takeaways / Actions

- Everyone is involved in Cures Act Final Rule compliance
- Policy and procedure development precedes training and implementation
- Clear, consistent and center-wide communication is key
- March will be a continuation of this presentation to focus on preparing for external communication and interoperability
- After the March session, you will receive an actionable checklist covering all February and March topics to assist in preparedness

Educational Series Schedule

Additional Ask the Experts sessions will be scheduled based on member interest. We welcome your suggestions! HCCN@chcanys.org

Month	Topic	Webinar Date	Ask the Experts (ATE) Date(s)	
November 2021	**Cures Act Overview**	**Wed, Nov 10** Noon-1 ET	All roles **Wed, Nov 17** Noon-1 ET	
December	**OpenNotes Overview**	**Wed, Dec 1** Noon-1 ET	Providers **Wed, Dec 15** Noon-1 ET	
January 2022	**Information Blocking Exceptions**	**Wed, Jan 12** Noon-1 ET	Compliance, HIM **Tue, Jan 18** Noon-1 ET	
February	**Preparing for Cures Act Regulatory Compliance, Part 1** (organizational readiness)	**Wed, Feb 16** Noon-1 ET	Compliance, HIM, IT **Wed, Feb 23** Noon-1 ET	
March	**Preparing for Cures Act Regulatory Compliance, Part 2** (communication of records)	**Wed, Mar 16** Noon-1 ET	Providers **Wed, Mar 23** Noon-1 ET	Compliance, HIM, IT **Wed, Mar 23** 2-3 ET

Before we move to Q&A…

Contact Info

Denise Webb

- Glidepath Consulting LLC
- Email: denise@glidepathconsulting.llc
- Phone: 608-358-9115

Jen Pincus

- CHCANYS- Project Director HCCN
- Email: jpincus@chcanys.org or hccn@chcanys.org
- Phone: 518-434-0767 x231

COMMUNITY HEALTH CARE ASSOCIATION of New York State

Appendix

Information Block Glossary of Terms

- **Actors**
  - Individuals and entities covered by the information blocking provision, i.e., health care providers, health IT developers of certified health IT, health information networks, and health information exchanges
- **Certified Health IT**
  - A health IT product that meets the certification requirements under the ONC Health IT Certification Program. Requirements for certification are established by standards, implementation specifications and certification criteria adopted by the Secretary at the Department of Health and Human Services (HHS)
- **Consumer Third-Party Application**
  - Applications developed by third parties authorized and used by patients to access, exchange and use their electronic health information

Information Block Glossary of Terms

- **Designated Record Set**
  - The set of information that a patient is required to have access to, such as medical and billing records, case management and health plan enrollment. Includes records that are used “to make decisions about individuals” also are included; this definition is not fully defined by the ONC but is addressed in an ONC FAQ
- **Electronic Access**
  - An internet-based method that makes EHI available at the time the electronic health information is requested and where no manual effort is required to fulfill the request
- **Electronic Health Information (EHI)**
  - The electronic protected health information (ePHI) in a designated record set (as defined in the Health Insurance Portability and Accountability Act (HIPAA) regulations) regardless of whether the records are used or maintained by or for a covered entity

Information Block Glossary of Terms

- **Health Information Network (HIN)/ Health Information Exchange (HIE)**
  - Individual or entity that determines, controls, or has discretion to administer any requirement, policy, or agreement that permits, enables, or requires the use of any technology for access, exchange, or use of EHI: (1) Among more than two unaffiliated individuals or entities (other than individual or entity to which this definition might apply) that are enabled to exchange with each other; and (2) Is for a treatment, payment, or health care operations (TPO) purpose regardless of whether individuals or entities are subject to 45 CFR 160 and 164
- **Health IT developer of certified health IT**
  - An individual or entity that develops or offers health information technology and which had, at the time it engaged in a practice that is the subject of an information blocking claim, health IT (one or more) certified under the ONC Health IT Certification Program

Information Block Glossary of Terms

- **Information Blocking**
  - If conducted by a health provider, a practice likely to interfere with access, exchange or use of electronic health information (EHI) when the provider knows that such practice is unreasonable and is likely to interfere with access, exchange or use of EHI
- **Interoperability**
  - Health information technology that (a) enables the secure exchange of electronic health information with, and use of electronic health information from, other health information technology without special effort on the part of the user; (b) allows for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable State or Federal law; and (c) does not constitute information blocking