ROCHESTER RHIO

Regional Health Information Organization

Survival Series: Enforcement of the Information Blocking Rules is Almost Here

What Providers Need to Know

Amy S. Warner, Esq., MBA
General Counsel, Privacy, & Compliance Officer
Rochester RHIO
amy.warner@grrhio.org

Denise DiNoto
Chief Engagement Officer
Rochester RHIO
denise.dinoto@grrhio.org

Disclaimer

ROCHESTER RHIO

- This material is designed to provide you with educational information about the new Information Blocking, or Information Sharing, rules.
- The presenters are not providing or offering legal advice but, rather, practical and useful information that could help individuals in the audience work within their organizations to try to achieve compliance with the Information Blocking rules.
- Every reasonable effort has been taken to ensure that the educational information provided is accurate and useful.
- Applying best practice solutions and achieving results will vary in each environment.

Agenda

- Introductions
- Rochester RHIO
- CURES Act Final Rule
- What Providers Need to Know
- Timeline, Penalties, and Exceptions
- Examples & Use Cases

Amy S. Warner, Esq.

Denise DiNoto

ROCHESTER RHIO

Reminder…

ROCHESTER RHIO

Generally speaking, patients cannot be denied access to medical records. (HIPAA)

Rochester RHIO (Regional Health Information Organization)

We provide electronic access and services for authorized medical providers, care managers, and appropriate community-based organizations with secure, electronic access to patient information:

- Lab reports, images, and radiology results
- Hospital discharge notifications with clinical reports
- Ambulatory care summaries
- Hospital admission/discharge notification
- Demographics, deceased notification, some SDOH
- Participation in health homes

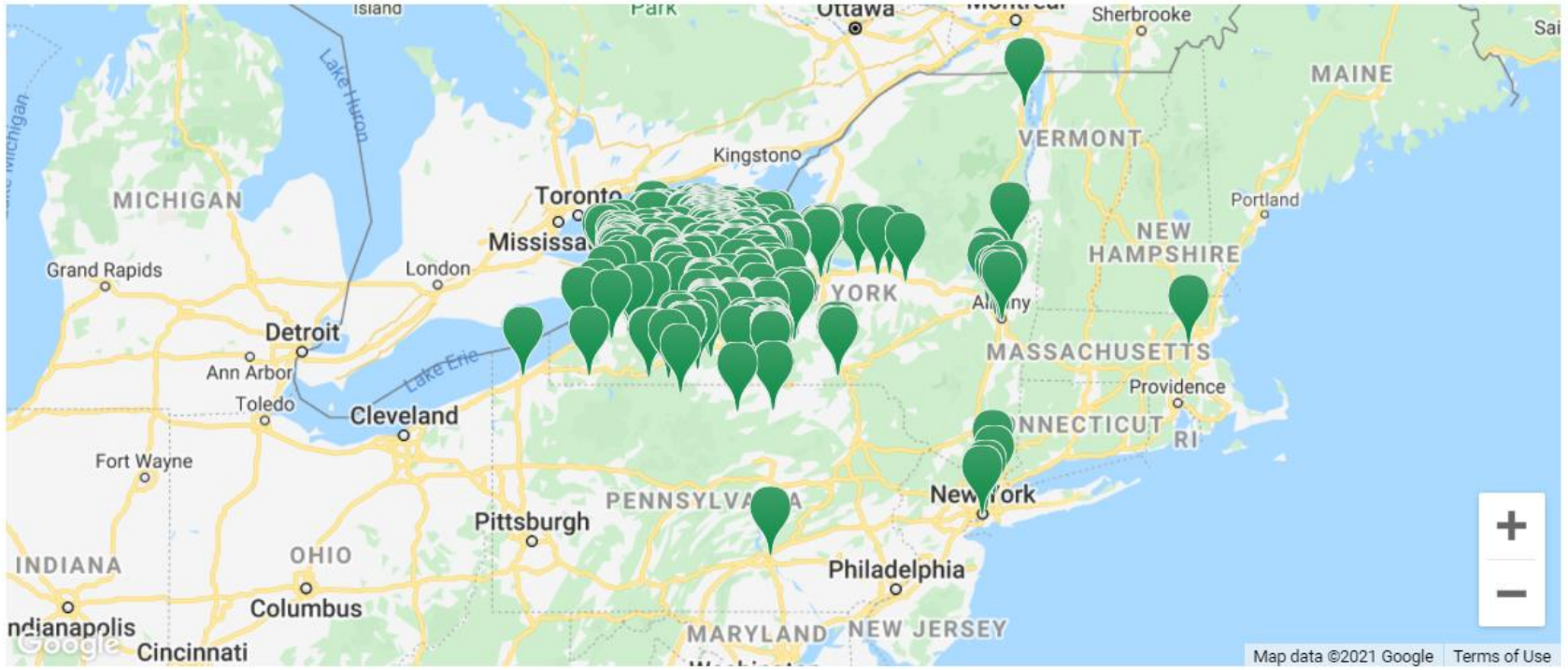
Photo by Edward Jenner from Pexels

More: https://providerportal.grrhio.org/ParticipantMap

Data Contribution

CONTRIBUTE

More than 1,000 practices contribute data to Rochester RHIO, including 23 regional hospitals and nearly 300 community-based organizations.



More: https://providerportal.grrhio.org/ParticipantMap

Rochester RHIO is Complying

ROCHESTER RHIO

- Patients can request a data file from Rochester RHIO

- https://rochesterrhio.org/access-my-health-data

- Required to educate patients on security risks

- Required to educate patients on privacy risks

ONC's Cures Act Final Rule

ROCHESTER RHIO

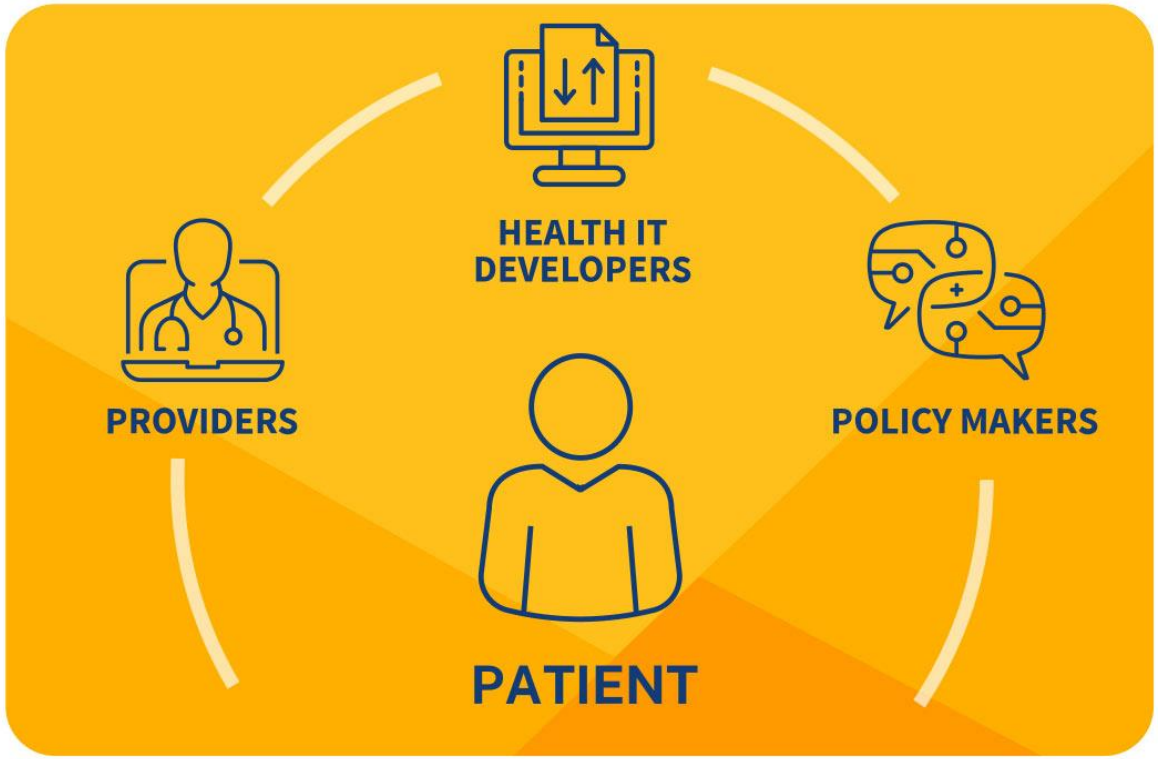
- Signed into law on 12-13-2016
- Interoperability of electronic health information, including patient access, is a major focus of the 21st Century Cures Act.
- Today's Focus: "Information Blocking, What Providers need to know.

Resource:
https://www.healthit.gov/curesrule/

Who Does This Apply To?

ROCHESTER RHIO

Applies to “Actors”, such as health care providers, certified health information technology vendors (EHR vendors) and HIE/HINs. (§4004)



Resource:
https://www.healthit.gov/curesrule/

Providers are “Actors” (Covered by the Rules)

- “Healthcare Provider” is defined to include nearly any entity rendering healthcare, including physicians, practitioners, laboratories, nurses, group practices, hospitals, long term care facilities, clinics, ambulatory surgery centers, administrators and other entities determined appropriate by HHS. 42 USC §300jj(3); 45 CFR §171.102

- Many Providers incorrectly believe that their EMR vendor is taking care of everything that a Provider needs to do to be in compliance with the Information Blocking Rule.

Resource: American Medical Association:
New information-blocking rules:
What doctors should know

What is Information Blocking?

ROCHESTER RHIO

- Information Blocking: An act or omission that "except as *required* by law or specified by the Secretary [in rulemaking], is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information [EHI]." (§4004)
- Information blocking applies to *any* request for EHI, for *any* purpose. HIPAA applies to any format of PHI.

Intent Matters (Knowledge Standard)

- If conducted by a certified health information technology vendor or a health information network or exchange, the entity "**knows or should know**" that the practice is likely to interfere…."
- If conducted by a health care provider, the providers "**knows**" the practice is unreasonable and likely to interfere…..

Definition of Electronic Health Information (EHI)

- EHI Defined: Protected electronic health information (EHI) that meets the HIPAA definition of “designated record set” (i.e., information that patients have the right to access).
- Designated record set is all information in the medical record plus information in other records that is used to make decisions about individuals.

Definition of Electronic Health Information (EHI)

- For the first 18 months the information blocking rules are in effect (until 10/6/2022), the definition of “EHI” is limited to the information in the U.S. Core Data Set for Interoperability (USCDI).
- Most USCDI data elements already captured in certified EHRs today, so information blocking policies APPLY to the data that's available in YOUR system today.

Resource: HITAC Standard Recommendations

US Core Data For Interoperability

The Office of the National Coordinator for Health Information Technology

Allergies and Intolerances *NEW

- Substance (Medication)
- Substance (Drug Class) *NEW
- Reaction *NEW

Assessment and Plan of Treatment

Care Team Members

Clinical Notes *NEW

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

Goals

Health Concerns

Immunizations

Laboratory

- Tests
- Values/Results

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 *NEW
- Previous Address *NEW
- Phone Number *NEW
- Phone Number Type *NEW
- Email Address *NEW

Problems

Procedures

Provenance *NEW

- Author Time Stamp
- Author Organization

Smoking Status

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) *NEW
- Weight-for-length Percentile (Birth - 36 Months) *NEW
- Occipital-frontal Head Circumference Percentile (Birth - 36 Months) *NEW

For more info:

HealthIT.gov/USCDI

New Data Elements for USCDI

ROCHESTER RHIO

Clinical Notes *NEW

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

Allergies and Intolerances *NEW

- Substance (Medication)
- Substance (Drug Class) *NEW
- Reaction *NEW

- BMI Percentile (2-20 years old) *NEW
- Weight-for-length Percentile (Birth - 36 months) *NEW
- Occipital-frontal Head Circumference Percentile (Birth - 36 months) *NEW

Provenance *NEW

- Author Time Stamp
- Author Organization

- Notes need be made available as soon as they are available electronically.
- Notes cannot be hidden or redacted, unless an exception is met. Exception: Psychotherapy notes
- Reminder: Possible that a parent may have access to a teen's confidential medical record because many EHRs do not segment data. Need to verify intent.
- Physicians need to create policies or processes around different scenarios:
  - Known or suspected child abuse
  - Complying with state or federal law
  - Preventing a parent from inappropriate access

Resource: American Medical Association

How doctors can adjust to new reality—opening notes to patients

Timeline and penalties

- Final Info. Blocking Rule published on May 1, 2020
- Vol. 85, No. 85: Federal Register
- **Rule goes into effect April 5, 2021**
- HHS Office of the Inspector General (OIG) can investigate cases of Info. Blocking & issue penalties of up to $1 M per violation against EHR vendors and HINs/HIEs. **(NOT Providers)**

Penalties (Provider Specific)

Unlike EHRs, HIEs or HINs, health care providers are not subject to the $1 million-per-violation CMPs under Section 4004 of the Cures Act.

- Congress directed OIG to refer provider violations to “the appropriate agency to be subject to appropriate disincentives using authorities under applicable Federal law, as the Secretary sets forth through notice and comment rulemaking.”
- HHS has yet to identify the agency or agencies that will handle information blocking referrals
- HHS has yet to identify the “disincentive” that will apply to providers that don’t share information.

Examples of Potential Violations

- Practices that restrict access, exchange or use of EHI authorized under applicable state/federal law for treatment and other permitted purposes. (Like General Policy Restriction)
- Implementing health IT in nonstandard ways that are likely to substantially increase the complexity/burden of accessing, exchanging or using EHI. (Like an Intentional Technical Limitation)
- Implementing IT in ways likely to restrict access/exchange/use of EHI with respect to exporting complete information sets or facilitating transitions between health IT systems. (Interference)
- Implementing IT in ways likely to lead to fraud, waste, abuse or impede innovations/advancement in EHI access/exchange or use. (Like Opportunistic Behavior)

Priority Areas From Rules

ROCHESTER RHIO

Info. Blocking “will almost always be implicated” when a practice “INTERFERES WITH” EHI for these purposes:

- Providing patients with access to their EHI and the ability to exchange and use it without special effort (also charging individuals a fee to electronically access their EHI)
- Ensuring health are professionals, caregivers, and other authorized persons have EHI for treatment and care coordination
- Ensuring payers get information they need to ”assess clinical value” and promote transparency of cost and quality of care
- Ensuring providers can get information for quality improvement and population health management activities
- Supporting access/exchange/use for patient safety and public health purposes.

Exceptions to Information Blocking

- The Cures Act authorized HHS to identify “reasonable and necessary activities” that do NOT constitute Information Blocking.
- Final Rule outlines 8 exceptions (“Safe Harbors”)
- Must satisfy ALL of the relevant conditions of each exception at all relevant times
- If you don’t meet an exception?
  - No guaranteed protection against penalties.
  - Each situation is evaluated on a case-by-case basis to see if “interference” truly occurred and if the behavior met the intent standard.

Information Blocking Exceptions

- Two Categories:
  - Group A: Exceptions involving **NOT** fulfilling requests of EHI
  - Group B: Exceptions involving procedures **for** fulfilling requests of EHI
- Each exception comes with conditions that **must** be met

A. Exceptions for NOT Fulfilling Requests

1. **Preventing Harm:** Reasonably necessary practices to prevent harm to a patient or another person.
2. **Privacy:** Refusing to fulfill a request to protect a person's privacy.
3. **Security:** Can interfere with the access/exchange/use of EHI to protect the security of EHI.
4. **Infeasibility:** Does not fulfill a request to access/exchange/use EHI due to the infeasibility of the request. (Written notification=10 days)
5. **Health IT Performance:** Reasonable, necessary measures to make health IT temporarily unavailable or degrade overall performance of health IT.

   Example: If an app is "hammering the database" or "disrupting others, it's okay to deny access," says Nick Hatt. "It's also okay to take scheduled downtimes."

B. Exceptions: Procedures FOR Fulfilling Requests

1. **Content & Manner:** Limiting content, manner in which an actor fulfills requests.
2. **Fees Exception:** Reasonable fees (including those that generate a reasonable profit),

BUT:

Cannot charge fees “based in any part on electronic access by an individual, their personal representative, or an entity designated by that individual to access the individual’s EHI.”

3. **Licensing Exception:** Actors may license interoperability elements for EHI to be accessed/exchanged/used.

Use Case: Responses to Individual Access

- Individual (or an app or service used by an individual) approaches your organization, or person who works there, to obtain EHI.
- How do you respond?

Possible responses:

- Fulfill request in the manner requested.
- Fulfill request in an alternative manner (See next slide).
- Don’t fill request – Is there an exception that applies?

Fulfilling Request: “Alternative Manner”

- Ordinarily, a request must be fulfilled “in the manner requested” unless “technically unable” or ”cannot reach agreeable terms” with requestor.
- If fulfilling in an alternative manner, must fulfill request “without unnecessary delay” in the following order of priority:
  - Using certified EHR technology;
  - Using content and transport standards specified by the requestor and published by the Federal Government or an ANSI-accredited standards developing organization;
  - Using an alternative machine-readable format, including the means to interpret the EHI, agreed upon with the requestor.
- If fulfilling in an Alternative Manner, must meet fee requirements (in this case, fees for electronic access by or on behalf of individuals are not permitted).
- If licensing of interoperability elements is involved, must meet licensure exception.

Declining a Request: Any Exceptions?

Example: Common Reasons to Decline

- Certified EHR Vendor does not possess/have access to information requested by the individual (USCDI for first 18 months)
- Provider no longer has access to the information.
- Contract with customers precludes responding
- Insufficient consent per state law. Does this fit the privacy exception?
- *Harm exception is not likely here unless a request meets the conditions for denial of right of access request under HIPAA. Note: Risk must be of* ***significant*** *physical harm.*

Infeasibility Exceptions

ROCHESTER RHIO

Designed to address “legitimate practical challenges”

- If claiming infeasibility, must respond within **10 business days** of receipt of the request as to why the request is infeasible (with a detailed written explanation).
- Conditions:
  - **Uncontrollable events:** The organization or person cannot fulfill the request due to a public health emergency, for example.
  - **Segmentation:** The organization or person cannot fulfill request because cannot you cannot unambiguously segment the requested EHI data from sensitive EHI that cannot be made available by law (or due to individual choice).

Infeasibility Exceptions

ROCHESTER RHIO

- Conditions, continued:

  Infeasible under the circumstances: The organization or person demonstrates, prior to responding to the request, in writing, the following factors that led to its infeasibility determination:

  A. The type of EHI and the purposes for which it may be needed;
  B. The cost of complying in the manner requested;
  C. The financial and technical resources available to you or your organization;
  D. Whether your practice is nondiscriminatory, and you, or your organization, provides the same access/exchange/use to its companies, suppliers, partners, and other persons with whom it has a business relationship;
  E. Whether you have control over the network through which EHI is exchanged; and
  F. Why you were unable to provide access/exchange/use by negotiating an alternative means.

Not an Infeasibility Exception

ROCHESTER RHIO

Not permitted to be considered as an exception: whether the manner requested facilitates competition, or if would have prevented the actor from charging a fee.

Additional Guidance: “Preamble” Language

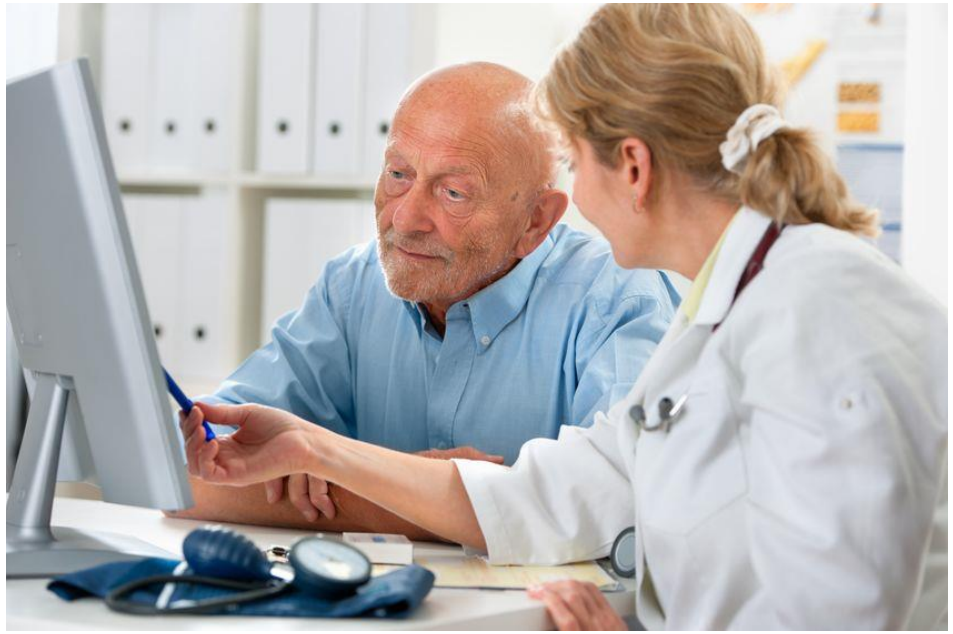
- “If an actor is permitted to provide [access/exchange/use] of EHI under the HIPAA Privacy Rule (or other law), then the Information Blocking provision would require the actor to provide that [access/exchange/use] as long as the actor is not prohibited by law from doing so (assuming no exception is available to the actor).”
- Re: BAAs: “While the Information Blocking rule does NOT require actors to violate these agreements, a BAA or its associated service level agreements must not be used in a discriminatory manner by an actor to forbid or limit disclosures that otherwise would be permitted by the Privacy Rule.”
- “To be clear, both the health care provider(s) who initiated the BAA and the BA who may be an actor…would be subject to the Information Blocking provision[s]….”

Additional Guidance: "Preamble" Language (2)

"The final rule supports an individual's ability to choose which third party developer and app are best for receiving all or part of their EHI.... [T]he final rule also supports and strongly encourages providing individuals with information that will assist them in making the best choices for themselves in selecting a third-party application."

Additional Guidance: “Preamble” Language (3)

“If an actor chooses not to provide [access/exchange/use] of EHI on the basis that the actor’s identity verification requirements have not been satisfied, the actor’s practice must be tailored to the specific privacy risk at issue…..
[T]his would require that the actor ensure that it does not impose identity verification requirements that are unreasonably onerous under the circumstances.”



Privacy Exception

ROCHESTER RHIO

Must meet ALL of the requirements of at least one of these subsections:

- If precondition not satisfied (if state/federal law requires consent, for example). Of note: if consent provided but doesn't meet all legal requirements, must help an individual submit a consent that complies with law and can't improperly encourage individual to withhold consent.
- If violates privacy policy of certified Health IT Developer not covered by HIPAA
- Can deny an individual's request based on a reason for denying an individual's right of access request under HIPAA.
- If respecting an individual's request NOT to share information.

Security Exception

ROCHESTER RHIO

Must meet conditions (a), (b), and (c) and one of either (d) or (e).

(a) The practice must be directly related to safeguarding the confidentiality, integrity, and availability of EHI;

(b) The practice must be tailored to the specific risk being addressed; and

(c) The practice must be implemented in a consistent and nondiscriminatory manner; AND

(d) If the practice implements an organizational policy, the policy must be in writing, directly respond to the security risk, align with consensus-based standards or best practice guidance, provide objective timeframes and other parameters for responding to & addressing security incidents – OR

(e) If actor is making a case-by-case determination, actor must make determination that:

i. The practice is necessary to mitigate risk to EHI,

ii. There are no reasonable alternatives to address the risk that are less likely to interfere with the access/exchange/use of EHI.

Wrap-Up: Best Practices

ROCHESTER RHIO

- Providers should develop policies for how to handle requests from a range of entities for a range of purposes: public health, research, business intelligence.
- Will need to undertake a similar inquiry for these requests
  - Fulfill in the manner requested
  - Fulfill in an alternate manner
  - Do not fulfill; determine if exception applies (and if not, documenting rationale for why not)
- Be prepared! Develop policies and procedures for anticipated use cases.

Getting Prepared

ROCHESTER RHIO

- √ - Read the Rules: 45 CFR §171.103
- √ - Establish a Compliance Team
- √ - Assess Systems for Barriers to Compliance
- √ - Remove Barriers to Complying with Info. Blocking Rule
- √ - Complete a Risk Analysis
- √ - Update policies and procedures
- √ - Train and educate staff
- √ - Test, Monitor and Audit

Proposed HIPAA Changes

ROCHESTER RHIO

- OCR Public Comment Deadline Extension: **May 6**
- **Proposed changes:**
  - Strengthening individual rights to their information (including electronic information)
  - Facilitating better access to family and caregiver involvement
  - Facilitating information for better care coordination and case management.

Contact Us

@RochesterRHIO

@rochester-rhio

Rochester RHIO www.RochesterRHIO.org
Support Center 877.865.7446 |
support@grrhio.org

Amy S. Warner, Esq., MBA
General Counsel, Privacy, & Compliance Officer
Tel: 585.481.2969 | Email:
amy.warner@grrhio.org

Denise DiNoto | Chief Engagement Officer
Tel: 585.481.2946 | Email:
denise.dinoto@grrhio.org