SUMMARY OF REGULATORY PROVISIONS AND ORGANIZATION ACTION STEPS

Information Blocking Toolkit for Medical Groups

CONTENTS

Introduction

Information Blocking was included in the 21st Century Cures Act of 2016. The Cures Act defined "information blocking" and authorized the Secretary of the Department of Health and Human Services (HHS) to identify, through rulemaking by the Office of the National Coordinator for Health Information Technology (ONC), "reasonable and necessary activities that do not constitute information blocking" and identified the HHS Office of Inspector General (OIG) as the office to investigate claims of information blocking. The Cures Act also prescribed penalties for information blocking and called on ONC to implement a complaint process for reporting information blocking and provides confidentiality protections for complaints.[1] This resource is intended to assist medical group leaders better understand the information blocking provisions and develop policies and procedures to comply with its requirements.[2]

What is Information Blocking?

In general, information blocking is an action by a health care provider, health IT developer of certified health IT, health information network (HIN), or health information exchange (HIE) that, except as required by law or specified by HHS as a reasonable and necessary activity, is likely to interfere with access, exchange, or use of electronic health information (EHI).

ONC has stated that an action would satisfy the information blocking provision's "likelihood" requirement if, under the circumstances, there is a **reasonably foreseeable risk that the action will interfere with access, exchange, or use of EHI**. In the final rule ONC explained that a policy or action that limits timely access to information in an appropriate electronic format creates a reasonably foreseeable likelihood of interfering with the use of the information. The agency noted that whether the risk of interference is reasonably foreseeable will depend on the particular facts and circumstances attending the action at issue.

As well, for health care providers, the standard is that the entity "knows that such action is unreasonable and is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information."

[1] This MGMA member-benefit information blocking resource is based primarily on language included in the ONC final rule: (RIN 0955–AA01) *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program* and drawn from information sheets and guidance documents found on the ONC website.

[2] Disclaimer: This MGMA resource is for educational purposes only. It is not intended as legal or consulting advice, or as a substitute for the advice of a legal professional. It is not intended to address all possible legal and other issues that may arise regarding information blocking and interoperability. Each medical group should consider its own unique circumstances and requirements when developing a compliance plan.

KEY POINT

A medical group may violate the information blocking rule if they knowingly take actions that interfere with exchange, access, and use of EHI, **even if no harm is caused**. A medical group, for example, may have a policy that restricts access to patient lab results for a certain amount of time to permit review by a clinician. Even if patients are not aware there is a delay, ONC is concerned that an action that is merely "likely" to interfere with the access, use, or exchange of EHI could be considered information blocking. Similarly, a medical group that has the capability to provide a patient same-day access to their results, but take several days to respond, could also be considered information blockers.

Definition of Electronic Health Information

For the first two years (currently defined as until October 6, 2022), medical groups must respond to a request to access, exchange, or use EHI with, at a minimum, the EHI identified in the United States Core Data for Interoperability Version 1 (USDCI).[3]

The USCDI data elements include:

Allergies and Intolerances
Represents harmful or undesirable physiological response associated with exposure to a substance.

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

Assessment and Plan of Treatment
Represents a health professional's conclusions and working assumptions that will guide treatment of the patient.

Care Team Member(s)
The specific person(s) who participate or are expected to participate in the care team.

[3] ONC has posted a comprehensive description of each the USCDI data elements here.

Clinical Notes

Composed of both structured (i.e. obtained via pick-list and/or check the box) and unstructured (free text) data. A clinical note may include the history, Review of Systems (ROS), physical data, assessment, diagnosis, plan of care and evaluation of plan, patient teaching and other relevant data points.

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

Goals

An expressed desired health state to be achieved by a subject of care (or family/group) over a period of time or at a specific point of time.

Health Concerns

Health related matter that is of interest, importance, or worry to someone who may be the patient, patient's family or patient's health care provider.

Immunizations

Record of an administration of a vaccination or a record of a vaccination as reported by a patient, a clinician, or another party.

Laboratory

- Tests
- Values/Results

Medications

Patient Demographics

- First Name
- Last Name
- Previous Name
- Middle Name (including middle initial)
- Suffix
- Birth Sex
- Date of Birth
- Race
- Ethnicity
- Preferred Language
- Current Address
- Previous Address
- Phone Number
- Phone Number Type
- Email Address

Problems

Information about a condition, diagnosis, or other event, situation, issue, or clinical concept that is documented.

Procedures

An activity that is performed with or on a patient as part of the provision of care.

Provenance

The metadata, or extra information about data, that can help answer questions such as when and who created the data.

- Author Time Stamp
- Author Organization

Smoking Status

Classification of a patient's smoking behavior.

Unique Device Identifier(s) for a Patient's Implantable Device(s)
A unique numeric or alphanumeric code that consists of a device identifier (DI) and a production identifier (PI).

Vital Signs
Physiologic measurements of a patient that indicate the status of the body's life sustaining functions.

- 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)

Note that medical groups are only required to report the data elements that they have captured. For example, it would not be considered information blocking if the patient's "smoking status" was not captured and thus not made available to the requestor.

On and after the initial two-year period, a medical group must respond to a request to access, exchange, or use EHI with EHI defined more broadly. This would include medical records, billing records, payment and claims records, case management records, and other records used, in whole or in part, by for a medical group to make decisions about individuals.

KEY POINT

EHI does not include:
- Psychotherapy notes
- Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding
- De-identified health information

Actions that could constitute information blocking

What makes a medical group a potential information blocker? The elements of information blocking include:

- The medical group is regulated by the information blocking provisions.
- The action involves EHI.
- The action is likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI.
- Knowledge of the action by the medical group.
- The action is not required by law.

ONC has identified potential actions that could constitute information blocking. These include:

- Limiting or restricting the interoperability of health IT, such as disabling or restricting the use of a capability that enables sharing EHI with users of other systems or restricting access to EHI by certain types of persons or purposes that are legally permissible or refusing to register a software application that enables patient access to their EHI (assuming there is not a legitimate security reason that meets the conditions of the Security Exception).
- Implementing health IT in ways that are likely to restrict the access, exchange, or use of EHI with respect to exporting complete information sets or in transitioning between health IT systems. This would include acts that make transitions between certified health information technologies more challenging (e.g., an EHR vendor charging excessive fees or using tactics to delay a action's switch from their EHR to another vendor's EHR).
- Restrictions on access, exchange, and use, such as may be expressed in contracts, license terms, EHI sharing policies, organizational policies or procedures or other instruments or documents that set forth requirements related to EHI or health IT, such as Business Associate Agreements (BAAs).

- Rent-seeking (e.g., gaining larger profits by manipulating economic conditions) or other opportunistic pricing actions.
- Any action that restricts authorized access, exchange, or use under applicable state or federal law of such information for treatment and other permitted purposes under such applicable law, including transitions between certified health information technologies.
- Implementing health IT in nonstandard ways that are likely to substantially increase the complexity or burden of accessing, exchanging, or using EHI.
- Implementing health IT in ways that are likely to—
  - Restrict the access, exchange, or use of EHI with respect to exporting complete information sets or in transitioning between health IT systems; or
  - Lead to fraud, waste, or abuse, or impede innovations and advancements in health information access, exchange, and use, including care delivery enabled by health IT.
- Internal policies or procedures that require staff to obtain an individual's written consent before sharing any of a patient's EHI with unaffiliated providers for treatment purposes even though obtaining an individual's consent is not required by state or federal law.
- Limiting or restricting the interoperability of Health IT. For example, the medical group only providing the production application programming interface (API) endpoint information to apps it specifically approves. This could prevent other applications—and patients that use them—from accessing data that should be made readily accessible via standardized APIs.
- A medical group has the capability to provide same-day access to EHI in a form and format requested by a patient or a patient's health care provider but takes several days to respond.[4]
- A health system insists that local physicians adopt its EHR platform, which provides limited connectivity with competing hospitals and facilities. The health system threatens to revoke admitting privileges for physicians that do not comply. Similar concerns would arise were a medical group to engage in discriminatory actions—such as imposing unnecessary and burdensome administrative, technical, contractual, or other requirements on certain persons or classes of persons—that interfere with access and exchange or EHI by frustrating or discouraging efforts to enable interoperability.
- A medical group imposes one set of fees and terms to establish interfaces or data sharing arrangements with several registries and exchanges but offers another more costly or significantly onerous set of terms to establish substantially similar interfaces and arrangements with an HIE or HIN that is used primarily by health plans that purchase health care services from the provider at negotiated reduced rates.

[4] Note that current HIPAA privacy regulations permit medical group up to 30 days to provide the patient access to their information, while information blocking requires action without unreasonable delay. MGMA has raised this inconsistency with HHS and we anticipate additional guidance in this area.

Information Blocking Exceptions

Section 4004 of the Cures Act defined actions that constitute information blocking and authorized the HHS Secretary to identify reasonable and necessary activities that do not constitute information blocking (referred to as "exceptions"). There are two categories of exceptions:

1. Exceptions that involve not fulfilling requests to access, exchange, or use EHI

Preventing Harm Exception

It will not be information blocking for a medical group to engage in actions that are reasonable and necessary to prevent harm to a patient or another person, provided certain conditions are met. Preventing Harm Exception Exceptions that involve not fulfilling requests to access, exchange, or use EHI Exceptions that involve procedures for fulfilling requests to access, exchange, or use EHI Privacy Exception Security Exception Infeasibility Exception Health IT Performance Exception Content and Manner Exception Fees Exception Licensing Exception

Objective of the Exception: *This exception recognizes that the public interest in protecting patients and other persons against unreasonable risks of harm can justify actions that are likely to interfere with access, exchange, or use of EHI.*

Key Conditions of the Exception:

- The medical group must hold a reasonable belief that the action will substantially reduce a risk of harm;
- The medical group's action must be no broader than necessary;
- The medical group's action must satisfy at least one condition from each of the following categories: type of risk, type of harm, and implementation basis; and
- The action must satisfy the condition concerning a patient right to request review of an individualized determination of risk of harm.

Privacy Exception

It will not be information blocking if a medical group does not fulfill a request to access, exchange, or use EHI in order to protect an individual's privacy, provided certain conditions are met.

Objective of the Exception: *This exception recognizes that if a medical group is permitted to provide access, exchange, or use of EHI under a privacy law, then the medical group should provide that access, exchange, or use. However, a medical group should not be required to use or disclose EHI in a way that is prohibited under state or federal privacy laws.*

Key Conditions of the Exception

To satisfy this exception, a medical group's privacy-protective action must meet at least one of the four sub-exceptions:

1. Precondition not satisfied: If a medical group is required by a state or federal law to satisfy a precondition (such as a patient consent or authorization) prior to providing access, exchange, or use of EHI, the medical group may choose not to provide access, exchange, or use of such EHI if the precondition has not been satisfied under certain circumstances. 2
2. Health IT developer of certified health IT not covered by HIPAA: If a health IT developer of certified health IT is not required to comply with the HIPAA Privacy Rule, they may choose to interfere with the access, exchange, or use of EHI for a privacy-protective purpose if certain conditions are met.
3. Denial of an individual's request for their EHI consistent with 45 CFR 164.524(a) (1) and (2): A medical group that is a covered entity or business associate may deny an individual's request for access to his or her EHI in the circumstances provided under 45 CFR 164.524(a) (1) and (2) of the HIPAA Privacy Rule.
4. Respecting an individual's request not to share information: A medical group may choose not to provide access, exchange, or use of an individual's EHI if doing so fulfills the wishes of the individual, provided certain conditions are met.

Security Exception

It will not be information blocking for a medical group to interfere with the access, exchange, or use of EHI in order to protect the security of EHI, provided certain conditions are met.

Objective of the Exception: This exception is intended to cover all legitimate security actions, but does not prescribe a maximum level of security or dictate a one-size-fits-all approach.

Key Conditions of the Exception:

- The action must be: (i) Directly related to safeguarding the confidentiality, integrity, and availability of EHI; (ii) Tailored to specific security risks; and (iii) Implemented in a consistent and non-discriminatory manner.
- The action must either implement a qualifying organizational security policy or implement a qualifying security determination.

Infeasibility Exception

It will not be information blocking if a medical group does not fulfill a request to access, exchange, or use EHI due to the infeasibility of the request, provided certain conditions are met.

Objective of the Exception: *This exception recognizes that legitimate practical challenges may limit a medical group's ability to comply with requests for access, exchange, or use of EHI. A medical group may not have — and may be unable to obtain — the requisite technological capabilities, legal rights, or other means necessary to enable access, exchange, or use.*

Key Conditions of the Exception:

- The action must meet one of the following conditions: Uncontrollable events: The medical group cannot fulfill the request for access, exchange, or use of electronic health information due to a natural or human-made disaster, public health emergency, public safety incident, war, terrorist attack, civil insurrection, strike or other labor unrest, telecommunication or internet service interruption, or act of military, civil or regulatory authority. Segmentation: The medical group cannot fulfill the request for access, exchange, or use of EHI because the medical group cannot unambiguously segment the requested EHI. Infeasibility under the circumstances: The medical group demonstrates through a contemporaneous written record or other documentation its consistent and non-discriminatory consideration of certain fmedical groups that led to its determination that complying with the request would be infeasible under the circumstances.
- The medical group must provide a written response to the requestor within 10 business days of receipt of the request with the reason(s) why the request is infeasible.

Health IT Performance Exception

It will not be information blocking for a medical group 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.

Objective of the Exception: *This exception recognizes that for health IT to perform properly and efficiently, it must be maintained, and in some instances improved, which may require that health IT be taken offline temporarily. Medical groups should not be deterred from taking 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 health IT.*

Key Conditions of the Exception:

- The action must: (i) Be implemented for a period of time no longer than necessary to achieve the maintenance or improvements for which the health IT was made unavailable or the health IT's performance degraded; (ii) Be implemented in a consistent and non-discriminatory manner; and (iii) Meet certain requirements if the unavailability or degradation is initiated by a health IT developer of certified health IT, HIE, or HIN.
- A medical group may take action against a third-party app that is negatively impacting the health IT's performance, provided that the action is: (i) For a period of time no longer than necessary to resolve any negative impacts; (ii) Implemented in a consistent and non-discriminatory manner; and (iii) Consistent with existing service level agreements, where applicable.
- If the unavailability is in response to a risk of harm or security risk, the medical group must only comply with the Preventing Harm or Security Exception, as applicable.

2. Exceptions that involve procedures for fulfilling requests to access, exchange, or use EHI

Content and Manner Exception

It will not be information blocking for a medical group 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. Exceptions that involve procedures for fulfilling requests to access, exchange, or use EHI.

Objective of the Exception: *This exception provides clarity and flexibility to medical groups concerning the required content (i.e., scope of EHI) of a medical group's response to a request to access, exchange, or use EHI and the manner in which the medical group may fulfill the request. This exception supports innovation and competition by allowing medical groups to first attempt to reach and maintain market negotiated terms for the access, exchange, and, use of EHI.*

To satisfy this exception, a medical group must meet both of these conditions: **Content** + **Manner**

Key Conditions of the Exception

Content Condition: Establishes the content an actor must provide in response to a request to access, exchange, or use EHI in order to satisfy the exception.

1. Up to 24 months after the publication date of the Cures Act final rule, an actor must respond to a request to access, exchange, or use EHI with, at a minimum, the EHI identified by the data elements represented in the USCDI standard.
2. On and after 24 months after the publication date of the Cures Act final rule, an actor must respond to a request to access, exchange, or use EHI with EHI as defined by law.

Manner Condition: Establishes the manner in which an actor must fulfill a request to access, exchange, or use EHI in order to satisfy this exception. An actor may need to fulfill a request in an alternative manner when the actor is:

- Technically unable to fulfill the request in any manner requested; or
- Cannot reach agreeable terms with the requestor to fulfill the request.

If a medical group fulfills a request in an alternative manner, such fulfillment must comply with the order of priority described in the manner condition and must satisfy the Fees Exception and Licensing Exception, as applicable.

*For health care providers, the standard is that the medical group "knows that such action is unreasonable and is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information." For health IT developers of certified health IT and health information networks (HINs) or health information exchanges (HIEs) the standard is that the medical group "knows, or should know, that such action is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information." In addition, we recommend review of the examples included in the Final Rule of what is and is not considered interference at **85 FR 25811**.*

Fees Exception

It will not be information blocking for a medical group to charge fees, including fees that result in a reasonable profit margin, for accessing, exchanging, or using EHI, provided certain conditions are met.

Objective of the Exception: *This exception enables medical groups to charge fees related to the development of technologies and provision of services that enhance interoperability, while not protecting rentseeking, opportunistic fees, and exclusionary actions that interfere with access, exchange, or use of EHI.*

Key Conditions of the Exception The action must:

- **Meet the basis for fees condition.** » For instance, the fees a medical group charges must: (i) Be based on objective and verifiable criteria that are uniformly applied for all similarly situated classes of persons or entities and requests. (ii) Be reasonably related to the medical group's costs of providing the type of access, exchange, or use of EHI. (iii) Not be based on whether the requestor or other person is a competitor, potential competitor, or will be using the EHI in a way that facilitates competition with the medical group.
- **Not be specifically excluded.** » For instance, the exception does not apply to: (i) A fee based in any part on the electronic access by an individual, their personal representative, or another person or entity designated by the individual to access the individual's EHI. (ii) A fee to perform an export of electronic health information via the capability of health IT certified to § 170.315(b)(10).
- Comply with Conditions of Certification in § 170.402(a)(4) (Assurances – certification to "EHI Export" criterion) or § 170.404 (API).

Licensing Exception

It will not be information blocking for a medical group to license interoperability elements for EHI to be accessed, exchanged, or used, provided certain conditions are met.

Objective of the Exception: *This exception allows medical groups to protect the value of their innovations and charge reasonable royalties in order to earn returns on the investments they have made to develop, maintain, and update those innovations.*

Key Conditions of the Exception The action must meet:

- The negotiating a license conditions: A medical group must begin license negotiations with the requestor within 10 business days from receipt of the request and negotiate a license within 30 business days from receipt of the request.
- The licensing conditions: » Scope of rights » Reasonable royalty » Non-discriminatory terms » Collateral terms » Non-disclosure agreement
- Additional conditions relating to the provision of interoperability elements.

KEY POINT

Warning Patients about Third-Party Apps

Patients are permitted to request that actions make their health information available to a third-party app designated by the patient themselves. There is concern that these apps may not be secure and they could compromise the confidentiality of the health information. In the 2020 final rule, however, ONC makes it clear that while the medical group can educate the patient and warn them about the potential dangers associated with releasing their health information to a third-party app, they cannot prevent the data from being accessed by the app.

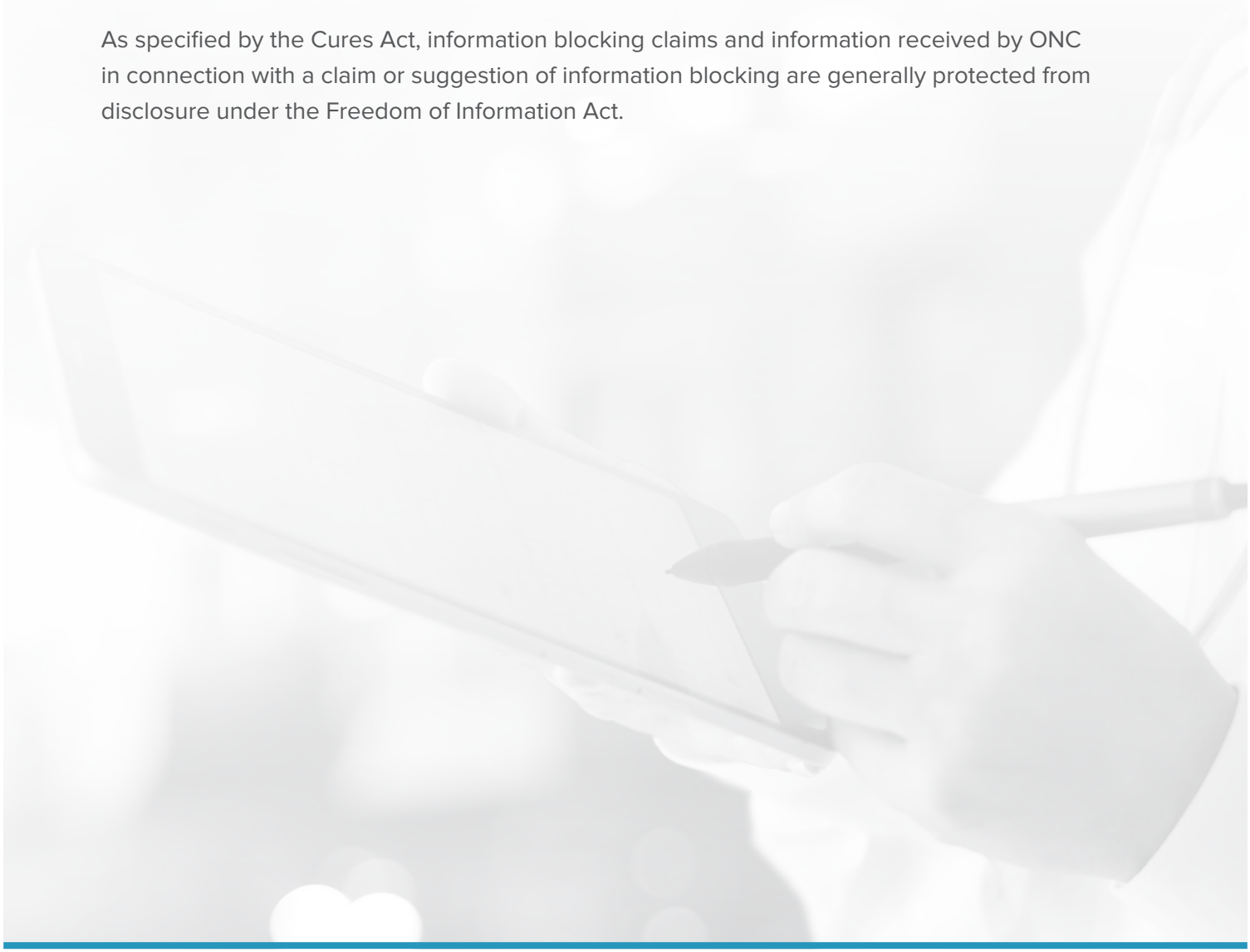
Potential Penalties

Section 4004 of the Cures Act defines a potential penalty of up to $1 million per violation for health IT developers and information networks determined by the Office of the Inspector General to have engaged in information blocking. Physician actions and other healthcare providers, on the other hand, will be referred to CMS if they have made a fraudulent attestation under the MIPS Promoting Interoperability Program or to the Office for Civil Rights if there is a potential HIPAA violation. We are expecting regulations from OIG outlining additional penalties for providers violating the information blocking rules.

How are information blocking complaint submitted to ONC?

Information blocking complaints can be submitted through ONC's online Health IT Feedback Form.

As specified by the Cures Act, information blocking claims and information received by ONC in connection with a claim or suggestion of information blocking are generally protected from disclosure under the Freedom of Information Act.



Medical Group Action Steps

01 **Designate a leader in your medical group.** With its impact on organizational operations and potential penalties for non-compliance, medical groups are encouraged to designate an individual within the organization to be the point person for both information blocking policy development and for any issues that arise from patient requests for EHI. In many cases this duty could be added to the organization's designated chief privacy officer.

02 **Review existing policies and procedures.** Medical groups are encouraged to complete a thorough review of all existing organizational policies and procedures for receiving, processing, and responding to requests to access, exchange, or use EHI.

03 **Coordinate with your health IT vendors.** Working with your EHR and online web portal vendors, identify and implement health IT policies or solutions that your organization needs to support patient EHI access requests or to comply with information blocking requirements.

04 **Review any fees charged patients.** Your organization should avoid charging patients (or persons or entities that they designate) requesting electronic access to their EHI through internet-based methods, such as personal health apps, personal health records, and email. In addition, ensure that any fees charged to individuals (or persons or entities that they designate) who request their EHI in physical media (such as paper copies, CD, or flash drive formats) comply with the requirements for reasonable, cost-based fees under HIPAA.[5]

05 **Evaluate all data use agreements and other agreements that could intersect with information blocking.** Medical groups may have agreements with heath IT vendors, local HIEs, hospitals, and other entities. These agreements should be reviewed to ensure they comply with the information blocking requirements.

06 **Revise current policies and procedures.** After reviewing all internal policies and procedures relating to EHI access, exchange, or use, revise them as necessary to ensure compliance with federal information blocking requirements. Similarly, medical groups should revise or create policies and procedures for responding to specific EHI requests. This process could also include creating standardized forms for receiving, processing, and responding to such requests and procedures specifying how access to EHI may be provided.

[5] For additional information on these fees, review the MGMA member-benefit resource: The Patient Right to their Medical Record: Format, Fees and other Requirements

07 **Establish a process to apply exceptions.** Medical groups do have the ability to restrict access to EHI permitted the restriction falls within one of the eight exceptions covered above. Groups should develop a process to review EHI requests from patients and ask the question should one of the exceptions be applied. ONC has indicated that it will be evaluating information blocking complaints and exception applications on a case-by-case basis. Groups seeking to apply one of the exceptions will need to fully document each case. MGMA has called on ONC to develop documentation templates to assist medical groups comply.

08 **Document all policies, procedures, and actions.** All policies developed by medical groups to comply with the information blocking requirements should be fully documented. Groups are encouraged to retain this documentation for at least six years from the date of its creation or the date when it was last in effect, whichever is later. In addition, any documentation created as part of an EHI request and/or the application of one or more of the exceptions should also be retained for at least six years.

09 **Train your staff.** Medical groups should train both administrative and clinical staff regarding their information blocking policies and the importance of adhering to the organization's information blocking policies. Groups should also consider regular training exercises that include discussions of actual patient EHI requests and how these were handled.

10 **Monitor MGMA for updates.** The federal government is expected to announce additional information blocking policies in 2021. As that guidance or additional regulatory language is released, MGMA will communicate those changes to members via the *Washington Connection* electronic newsletter and will be updating this resource to include this new information. Medical group leaders are encouraged to monitor MGMA communications for updated information blocking policies and resources.

INFORMATION BLOCKING TOOLKIT FOR MEDICAL GROUPS

MGMA
Medical Group Management Association®