AMA
AMERICAN MEDICAL ASSOCIATION

PART 2

How do I comply with info blocking and where do I start?

Doing what is best for the patient should always be front and center. Physicians have a responsibility to provide for the delivery of high-quality and safe patient care, a responsibility to provide patient care that meets professional standards, and a responsibility to advocate for the best interest of patients. Info blocking should not be viewed as "black or white"; it is okay to consider your patient's needs while thinking about compliance. **Physicians should strike a balance between strict regulatory compliance and exercising his/her independent professional judgment—guided by personal and professional beliefs—as to what is in the best interests of patients, the profession, and the community**.[1] When thinking about your compliance program, consider developing and documenting responses to the following: actions that you and your colleagues would identify as compromising medical judgment; what is in the best interest of your patient population; and policies and procedures that support individual patients' circumstances.

Where do I start?

You should start by identifying whether your organization already has a compliance program, even if it has not yet begun to work on info blocking compliance.[2] This is important because your existing compliance program will have structure, policies, procedures, and resources that will lay the foundation for info blocking compliance. Info blocking regulations and requirements are new for everyone; do not be surprised if your organization's compliance professionals are not knowledgeable about the info blocking rule. If your organization does not have a compliance program, then it is important to stand one up—both for info blocking compliance and for compliance with laws like HIPAA. Consider including these subject-matter experts within your organization:

- Legal counsel with health care expertise and who is knowledgeable about the info blocking law and regulations.
- IT expertise with understanding of how your organization controls access, exchange and use of EHI.
- Information privacy expertise with understanding of how your organization protects the privacy of EHI. This will include your privacy officer and others involved in HIPAA and state privacy law compliance.

You should consider starting with your organization's policies that currently address requests for access, exchange, or use of patient medical information. This is particularly important for situations where patients or their non-clinical caregivers are requesting electronic information. **Medical practices are urged to review**

1. https://policysearch.ama-assn.org/policyfinder/detail/guided%20by%20personal%20and%20professional%20beliefs?uri=%2FAMA-Doc%2FHOD.xml-0-2034.xml
2. To meet ONC's Information Blocking rules and regulations by the enforcement date, make sure your compliance program is established by April 5, 2021.

all policies related to their responses to information requests and update their policies and procedures as needed. This should include both HIPAA policies and those governing confidential or sensitive patient information, including information related to adolescent health. **Your policies must address each of the info blocking exceptions prior to the exception's use.** You should detail how each exception can be met to ensure that the exception is applied as narrowly as possible and in a non-discriminatory manner.

Critically, you should consider defining your organization's *reasonableness* standard. To be an info blocker, the law requires that physicians must **know that the practice is unreasonable** and likely to interfere with, prevent, or discourage access, exchange, or use of EHI. Developing and documenting scenarios where physicians may or may not take reasonable actions could assist in compliance audits. Procedures should provide a detailed workflow where case-by-case findings will be documented and by whom. Again, your HIPAA policies and procedures should also be aligned with info blocking requirements and consider any relevant state laws.

Moreover, ONC's rule requires all physicians to make their office notes, lab results, and other diagnostic reports available to patients as soon as the physician's office receives an electronic copy. Physicians across a wide range of specialties and practice types already have well-established protocols for the release of information. In circumstances such as genetic tests, adolescent health, mental health, and substance use disorder, physicians should consider how their organization's policies can incorporate important situational context each physician already uses in their day-to-day practice. For instance, consider these situations:

- **Situations related to the release of lab tests prior to physician review.** While a company-wide policy blocking patient access until a physician has a chance to review results would likely implicate the information blocking provision of ONC's rule, can a policy be created that enables physicians to consider the release of lab tests on a case-by-case basis? Such policy may take into account the physician's relationship with the patient, context of the reason for the lab test itself, who other than the patient may have access to the test results, and their medical specialty's guidelines around the release of information. Consider how a physician would document their decision to restrict access to information in accordance with their organization's policies and their profession's guidelines. While the Harm Exception does not allow physicians to use their concern for a patient's *emotional* harm as a reason to restrict access, how would a physician document—using their professional judgment—that their actions were **reasonable** given the circumstances?
- **Situations where sensitive information cannot be hidden or redacted from an office note.** In many instances, documenting a teen's confidential information within their medical record means that their proxy or parent may also have access. Many teens' EHR portals are established by their parents who would then have access to office notes, labs, and other sensitive information. EHRs often do not segment information based on who is accessing the patient's portal. ONC's Rule includes an exception (the Infeasibility Exception) for situations where information cannot be unambiguously segmented from a record. While that exception requires strict adherence to several conditions, including linking back to the Harm Exception, consider creating policies that outline how physicians should account for situations such as:
    - Known or suspected child abuse;
    - Respecting the patient's wishes about keeping information confidential;
    - Complying with state or federal law;
    - Preventing a parent from inappropriately accessing a child's confidential information;
    - Protecting the patient's privacy and confidentiality; and
    - Issues related to the complexity, cost, and burden of manually editing or hiding text in adolescent EHR records.

  Your organization may consider creating policies and procedures that reflect a physicians' desire to do what is best for the patient while exercising his/her independent professional judgment.

Part 2: How do I comply with info blocking and where do I start?

Physician organizations should identify and document where all patient EHI is held within the organization. While the EHR may hold the majority of your patients' medical records, you should also consider other health IT systems such as picture archiving and communication systems (PACS), practice management systems (PMS), and in-office laboratory systems or other diagnostic services owned or operated by the organization. These too may be subject to EHI requests.

Also, contemporaneous documentation of your use of an exception is always preferable to retrospective documentation. You should consider creating exception templates and customizable forms that match your organization's policies and procedures. Make sure all medical and office staff can easily access these documents. Also, consider asking your EHR vendor to incorporate these templates and make them easily accessible within the physician's workflow. This may simplify the process of documentation and provide better integration within your day-to-day practice.

Lastly, ONC makes clear that an Actor's failure to meet an exception does not automatically mean that the Actor engaged in info blocking. Just because there is no relevant exception, or a physician fails to meet all requirements of an applicable exception, does not mean that the physician will necessarily be found to have engaged in info blocking. The federal body tasked with enforcement and investigations—the Office of the Inspector General (OIG)—must still determine that the action taken by the physician meets the definition of info blocking.

Additional questions to consider:

- How does my organization access, exchange or use EHI? Start with those that impact patient or non-clinical caregiver access to records.
- What are the potential technological challenges requesters may face accessing, exchanging, and using EHI stored at my organization? **Pay particular attention to patient and non-clinical caregiver requests.**
- How long does it take to assess whether access, exchange, or use of EHI is granted?
    - For example, many physician organizations restrict patient access of some lab results or other diagnostic reports before a physician has an opportunity to review the result. Often there is a 36- to 48-hour window between patient access and when physicians have a chance to review. However, ONC's regulations define info blocking as an action by an Actor [physician] interfering with, preventing, or materially discouraging access, exchange, or use of EHI. Slowing or delaying access, exchange, or use of EHI could constitute an "interference" and implicate info blocking. Physicians who have the capability to provide a patient same-day access to their results, but take several days to respond, would likely be considered info blockers. However, always consider what is best for the patient and ensure your organizational policies and procedures reflect this. Also, how does your organization define accuracy with respect to office notes? Prematurely releasing inaccurate information, such as incomplete office notes, may cause harm to a patient. If an office note is not considered accurate until a physician signs off and takes action to release the note to the patient's portal, consider how your organization's policies and procedures could incorporate the Harm Exception for these situations.
- What types of practices does my organization engage in that appear on the list of examples of suspect practices?
    - For all legitimate practices that you identify, are there info blocking exceptions you can assert to prevent these practices from being considered prohibited Info blocking? Remember, you must meet **ALL** the conditions listed for a particular exception to meet that exception.
- What practices can you identify that your organization engages in that **do not** fit within an exception? Can you modify these practices to fit within an exception?

- For any practices that do not fit within an exception but are necessary for your business, can you document that your organization does not intend for these practices to result in info blocking? Recall that physicians must have the required ***knowledge and intent*** to interfere with access, exchange, or use of EHI to be considered info blockers.

Maintaining a compliance program

An effective compliance program, just like any program, requires routine review and maintenance. You should never simply download a stock compliance plan off the Internet and put it on the shelf without tailoring it to your organization (nor should you download it, tailor it, and then fail to use it!). No matter how your organization develops its info blocking compliance plan, it will require that you regularly review the program and test it. You should also tailor your program to suit your organization's size, resources, and culture. You will also want to keep a documented history of evaluating your compliance plan over time.

Conduct regular training on info blocking topics. This is a new requirement, and many staff will not understand the requirements. Make sure to keep records of staff attendance. Consider staring with short training sessions focused on specific topics or exceptions—then building on top of previous sessions throughout the training process.

Also, EHR vendors are likely to play a key role in info blocking compliance—or non-compliance. An effective info blocking compliance program should include the careful and considered evaluation of vendors that are involved in the access, exchange, or use of EHI. Additionally, Your EHR vendor may already have created resources or training modules to help with your compliance. Consider reaching out to your EHR vendor sooner than later.

Organizational risks

Not only is a compliance program an important component in making sure you and your organization meets the requirements of info blocking regulations, but it also will help defend your organization from info blocking complaints and any resulting OIG investigations. **Simply asserting that you were not aware or understood info blocking requirements is not a defense and would likely still result in penalties and disincentives from the federal government.** Additional organizational risks may include:

- Stiff fines and penalties (varied by Actor-type);
- Reputational risk;
- Implementation and compliance costs;
- Enforcement and regulatory uncertainty and conflicts (e.g., Cures vs. HIPAA);
- High volumes of information requests; and
- Audits may show that what seemed compliant was not and can expose you to unexpected liability. The OIG may refer investigative cases or findings to other federal agencies, including the Centers for Medicare and Medicaid Services or the Office of Civil Rights (e.g., issues related to HIPAA compliance).

Physicians should review all implementation and compliance issues and plan for the worst-case scenario. Exceptions will require new and updated policies and procedures—requiring you to embed them in your everyday workflows. You can also expect the rule to be "weaponized" by those seeking data access. We expect entities such as payers and health plans to leverage the info blocking rules to gain increased access to your EHR and patient records. While this may be communicated to you or your organization as a way to reduce administrative burden (e.g., reduce the burden around prior authorizations), there is increasing concern that payers could threaten physician practices with "info blocking action" if their requests for direct access into your EHR is denied. Payers having unfettered access to all your patients' records may impact patient coverage, access to care, narrowing of networks, or your autonomy to practice medicine. We strongly urge all physicians to seek counsel from an attorney prior to responding to any payer or health plan requests for direct access into your EHR.

Next steps

The info blocking regulations are very complex and will take time to fully implement and understand. Many health care systems, medical professional associations, and experts in compliance are still seeking clarity and guidance from the federal government. While the OIG has stated that it "will not bring enforcement actions against Actors who OIG determined made innocent mistakes," consider how your organization will stand up a compliance program, document your actions, and importantly, consider how your practices can be improved to better respond to patient requests for their data. Consider taking these as your first steps in complying with info blocking:

- Ask for information from your EHR vendor on their preparations for complying with the info blocking rules. Make sure your EHR vendor has a plan in place to distinguish between data elements included in the USCDI and other EHI included in the EHR for purposes of responding to requests for EHI. Ask how your EHR vendor will help you determine and document the use of exceptions.
- Consider whether and how your EHR will support data segmentation (e.g., based on a patient's preference or because protected EHI cannot separated from the office note to comply with state or federal law) and when the Infeasibility and/or Privacy Exceptions should be used.
- Evaluate whether your existing policies regarding an individual's right to access ePHI reflect the HIPAA Privacy Rule **AND** the ONC Final Rule. Reconciling HIPAA and ONC's Rules will take longer than expected; consider the need for additional resources, legal counsel, and assistance from compliance personnel.
- Consider adopting a new policy regarding denial of access to prevent harms, such as death or bodily harm.
- Consider defining your organization's reasonableness standard.
- **Review your organization's approach to staff training.** Your back and front office staff will often be the first to encounter EHI requests. They should have a clear understanding of your organization's obligations, policies and procedures, know how to respond (or not respond), and how to document which actions were taken and why. Document all staff trainings, including who attends and what was discussed.
- Review existing privacy and security policies addressing access to EHI, including policies on verifying the identity of persons and entities requesting EHI to determine whether they comply with the Privacy or Security Exceptions.
- Consider contacting your medical specialty association or state society and ask if they offer guidelines for responding to requests for medical records. For instance, some states have specific requirements around patients accessing labs or test results. Your medical specialty may also have guidelines on the release of information prior to a physician's review or recommendations around counseling, such as in terms of genetic test results. **Including these guidelines within your organization's policies and procedures—AND documenting how the use of an exception aligns with your state or specialty guidelines—may strengthen your compliance with the info blocking requirements.**
- Review policies and procedures addressing an individual's right under the HIPAA Privacy Rule to request additional restrictions on the use and disclosure of PHI to determine whether they comply with the Privacy Exception's sub-exception for an individual's request not to share EHI. Your state society may also be familiar with any particular state laws around privacy and sensitive information such as adolescent health, HIV or other STIs, and mental health.
- Review online privacy policies and other notices disclosed to individuals relating to EHI to determine whether the policies and notices are tailored to specific privacy risks. Confirm that your organization has properly implemented compliance with the policies.
- Consider whether to update existing information security risk assessment tools, policies and practices to require consideration of whether a potential security measure is tailored to specific security risks (i.e., security threat and vulnerability combinations) identified in the assessment, and whether there are reasonable alternatives that reduce risk of info blocking.

- Review existing security measures and policies concerning access to EHI by third-party requestors to determine whether they are directly responsive and tailored to security risks identified and assessed by or for the Actor.
- Consider adopting policies and procedures for evaluating and responding to potentially infeasible requests for EHI, including requests during public health emergencies or other uncontrollable events.

Additional resources

Federal government resources:

- Fact Sheets
- Recorded Webinars
- What ONC's Cures Act Final Rule Means for Clinicians and Hospitals
- What ONC's Cures Act Final Rule Means for Patients
- Link to ONC's Cures Act Final Rule
- Link to ONC's Information Blocking FAQs

Stakeholder coalition resources:

- The Sequoia Project Information Blocking Resource Center

Professional association resources:

- College of Healthcare Information Management Executives (CHIME)

Additional AMA resources:

- Summary of ONC's info blocking, interoperability, and EHR certification Final Rule