Information Blocking Rule: Basics and Considerations for Pediatric Practices

In May 2020, the federal Office of the National Coordinator for Health IT (ONC) published the 21st Century Cures Act Final Rule, usually referred to as the "Information Blocking Rule." After a delay related to the COVID-19 pandemic, the rule took effect on April 5, 2021. The rule seeks to promote the free flow of patient data, including empowering patients to have access to their own information.

While the Information Blocking Rule holds many benefits for patients and physicians, it raises some specific considerations for pediatric practices. Those practices may hold confidential data related to, for example, teen reproductive health, sensitive family situations, or adolescent mental health treatment. The rule, however, allows for physicians to keep this information confidential, provided that practices take the proper steps to implement their compliance efforts.

This summary is intended to help pediatricians understand the Information Blocking Rule, and how they can best interact with their patients and their families.

Understanding "Information Blocking"

As defined in the 21st Century Cures Act, Information Blocking is a practice that is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information. Put another way, information blocking is any action that a physician, hospital, health information organization (HIO), or health IT vendor takes that impedes the flow of electronic health information (eHI) to a patient or other person authorized to request it.

Some examples of actions that could be considered information blocking include:

- Physicians or hospitals creating artificial barriers to data exchange, such as consent policies above what is required by HIPAA and CMIA.
- Providers attempting to "lock" patients into a particular system by refusing to release their data to other providers.
- Health IT vendors charging excessive fees for interfaces required for data exchange.

EFFECTS OF THE INFORMATION BLOCKING RULE ON PHYSICIAN PRACTICES

+ **Release of Patient Data:** Starting on April 5, 2021, physicians are required to respond to any legitimate request to exchange or provide access to electronic health information (EHI) stored in their EHR. Such a request could come from a patient, another provider (for the purposes of treatment), a health plan (seeking information for clinical purposes), or a public health agency. Initially, EHI is limited to a certain set of data, but must be provided in the form requested.

  From April 2021 until October 6, 2022, the data that must be made available is the US Core Data for Interoperability (USCDI) version 1. See the complete set of USCDI data here. Beginning in October 2022, physicians will be expected to make all EHI held on the patient available.

  The most common concern CMA has heard from physicians regards the release of clinical notes – both structured and unstructured (not including psychiatric notes). Those notes must now be made available to the patient upon request, unless one of the exceptions listed in the next section below applies.

+ **Benefits for Physician Practices:** While the Information Blocking Rule creates new obligations for practices, it also provides substantial benefits for physicians and their patients.

  - **AVAILABILITY OF PATIENT DATA AT THE POINT OF CARE:** As hospitals, health plans, and other actors in the system make their data available, physicians will have more information at their disposal at the point of care. This will provide physicians with a more complete view of their patients, empowering higher quality care.
  - **PATIENT ENGAGEMENT IN THEIR OWN CARE:** As patients gain more access to their own data, they can become more active partners in their own health care.
  - **LOWERING THE COST OF DATA EXCHANGE:** One of the most common issues CMA hears from physicians with regards to data exchange is the excessive fees that EHR vendors and other health IT companies charge for the interfaces needed for health information exchange. With the implementation of this rule, those fees – if found to be truly excessive - could constitute information blocking.

+ **Penalties**: For the moment, there are no penalties for physicians who are found to be information blocking. The final rule only stipulates penalties for health IT vendors (up to $1 million per instance) and Health Information Exchanges/Networks. However, sometime in 2021 or 2022 there will be a subsequent rulemaking that lays out proposed penalties for physicians and other providers. CMA will distribute information about that rulemaking when it is available.

EXCEPTIONS TO THE INFORMATION BLOCKING RULE

The ONC has defined eight exceptions that allow physicians to restrict access to patient information without it constituting information blocking:

1. **Preventing harm exception –** The physician believes that there is a risk the patient will come to physical harm if the data is released.
2. **Privacy exception –** Generally, this applies to situations where releasing information could result in violating HIPAA or state privacy laws (such as the Confidentiality of Medical Information Act in California).
3. **Security exception –** The Security exception applies when the practice believes that the release of the data would compromise the security thereof.
4. **Infeasibility exception –** This exception covers uncontrollable events (such as wildfires) as well as technical reasons (such as the inability of the EHR to separate data from data that cannot be released due to privacy laws).
5. **Health IT performance exception -** This exception covers cases where a health IT system is offline for scheduled or unscheduled reasons.
6. **Content and manner exception –** As noted above, until October 2022, physicians are only required to release data in the USCDI. This exception covers data requests outside of that set. Physicians should discuss this exception with their EHR vendor.
7. **Fees exception –** Practices are allowed to charge reasonable fees for providing data. This mostly applies to EHRs and HIEs.
8. **Licensing exception –** This exception also applies mostly to EHRs. It allows vendors to license technology without it constituting information blocking.

For more information and detail on the 8 exceptions, please see the website of the Office of the National Coordinator for Health IT.

Special Considerations for Pediatric Practices

CMA has heard concerns from many pediatricians regarding the privacy of very sensitive data they hold about their patients, such as teen mental and reproductive health data, sensitive family issues (abusive and/or non-custodial parents), and substance abuse. Many pediatricians are concerned that the Information Blocking Rule will force them to release this data, especially if it is included in clinical notes. With the proper planning and safeguards in place, however, that does not need to be the case. The Privacy Exception, listed above, provides several routes for physicians to withhold sensitive information in the interest of protecting the privacy of their patients.

THE PRIVACY EXCEPTION – RESPECTING AN INDIVIDUAL'S WISH NOT TO SHARE INFORMATION

The Privacy Exception contains a sub-exception that allows physicians not to allow access, exchange, or use of a patient's health information based on the patient's wishes.

The patient must make this determination without any coercion or encouragement from their physician. And, as is the case with all exceptions, it must be applied in a non-discriminatory manner.

If a patient requests that a physician no allow access to certain data, the physician should document that request as soon as possible. The patient can withdraw the request at any time either verbally or in writing.

THE PRIVACY EXCEPTION – CALIFORNIA STATE LAW

As noted above, the Privacy Exception to the Information Blocking Rule stipulates that a physician may withhold access to data based on state and federal privacy law. California has some of the strongest patient privacy laws of any state of the country. Some of the most important laws for pediatric practices to know:

- **Civil Code Section 56 – The Confidentiality of Medical Information Act (CMIA):** CMIA is California's main state-level privacy law governing the use of patient data. In general, CMIA prohibits the release of patient data without patient consent, unless the data is being used for treatment, to health plans for the purposes or payments, or for legal proceedings.
- **Health and Safety Code Section 123115 – Physician Discretion Regarding Release of Patient Records:** This code section states that the parent of a minor shall not have access to the minor patient's records "*Where the health care provider determines that access to the patient records requested by the representative would have a detrimental effect on the provider's professional relationship with the minor patient or the minor's physical safety or psychological well-being.*" This broad code section allows physicians discretion over whether to release the data of minor patients.
- **Health and Safety Code Section 124260 – Mental Health Treatment of Minors:** This section allows physicians not to include the parents of a minor patient in the patient's care if the physician deems that involvement would be inappropriate.

For more information on California Law related to patient access to data, see the following CMA health law library documents:

- #4205: "Patient Access to Medical Records"
- #4207: "Requests by Other Third Parties: CMIA, IIPPA and the HIPAA Privacy Rule"
- #4000: "Medical Records: Most Commonly Asked Questions"

UTILIZING AN EXCEPTION

To utilize an exception, practices must have written policies in place regarding how they react to requests for patient data. And the use of an exception must be assessed on a case-by-case basis. This article from the Journal of the American Health Information Management Association provides some helpful tips on how to develop your policies.

In addition, those exceptions must be applied in a non-discriminatory fashion. For example, a practice could elect not to release data related to teen reproductive health. They could not, however, elect to release that data for their patients who identify as male, but not for patients who identify as female. Policies must be applied equally across all patients.

Steps Practices Can Take

First, if your EHR vendor has not proactively informed you of their plans for coming into compliance with the Information Blocking Rule, you should contact them as soon as possible and ask for that information. It is very likely that your EHR system may need updates or add-ons, so you will want to get in the queue for those as soon as possible.

One important question you will want to ask your EHR vendor is about data segmentation. Your EHR system may allow you to designate some patient data (that falls under one of the exceptions listed above) as confidential and withhold it from a release of patient data. If your EHR does allow for this segmentation, you need to familiarize yourself and your staff with how to utilize that function.

Once you have done that, you will want to review your internal processes for responding to requests for patient information, both from patients and other providers. Any workflow process that you have that inhibits access to information should be reviewed very carefully. For example, if you routinely hold lab results for a set amount of time, that could be information blocking. Depending on your situation, you may wish to consult an attorney with expertise in privacy and security rules.

Finally, physicians may wish to consider what is included in your clinical notes. Going forward, physicians must write notes assuming that they may be read by the patient or someone else authorized to request them. It can be helpful to use clear, concise language and avoid jargon ("follow up" as opposed to "F/U"). Physicians may also wish to include more context in their notes to allow patients to understand them better.

Additional Resources

- The Office of the National Coordinator for Health IT has many resources on information blocking: healthit.gov/topic/information-blocking
- In addition, the American Medical Association has developed several guides for physicians on how to comply with the rule: ama-assn.org/practice-management/digital/new-information-blocking-rules-what-doctors-should-know
- On February 18, 2021, CMA held a webinar in conjunction with the ONC for California physicians: cmadocs.org/store/info/productcd/CMA21_0218_INFO/t.
- "Impact of 21st Century Cures Act interoperability rule on pediatric clinicians," AAP News, April 1, 2021. aappublications.org/news/2021/04/01/hit040121.

STAFF CONTACT: David T. Ford
Vice President, Health Information Technology
(916) 444-5532
dford@cmadocs.org