**CURES ACT (INFORMATION BLOCKING) RULE BASICS FOR PROVIDERS AND CLINICAL STAFF**

In 2020, the Office of the National Coordinator for Health IT (ONC) released the Cures Act final rule regulating: (1) the certification criteria under the voluntary program for certification of Health IT modules, (2) the conduct of developers participating in the certification program, and **(3) the electronic sharing of health information (i.e., information blocking regulations).**

The information blocking (IB) section of the rule that regulates the sharing of electronic health information (EHI) was applicable to healthcare providers **beginning April 5, 2021**. This includes all healthcare entities and individual provider types and specialties as defined in the Public Services Act (42 U.S.C. 300jj) (i.e., hospital, clinic, FQHC, pharmacy, lab, MD, DO, RN, PA, APNP, pharmacist, dentist, therapist, social worker, etc.). The exceptions to fulfilling requests for access, exchange, or use of EHI provided in the Cures Act rule align with or are in addition to the HIPAA privacy and security rule requirements for the protection of, release of, and right of access to protected health information. The HHS OIG will start investigating claims of information blocking occurring beginning on September 1, 2023. Providers are not subject to OIG civil monetary penalties, but HHS will be issuing a proposed rule for public comment before the end of 2023 to establish appropriate disincentives for providers determined to be information blocking. The OIG will evaluate IB claims on a case-by-case basis and consider the individual facts and circumstances for level of impact, intent, and knowledge.

The Information Blocking section of the rule applies to any Patient's health records maintained electronically made by or for your organization. This includes medical and billing records and other records used in whole or in part to make decisions about individuals to the extent the records would be included in your organization’s Designated Record Set (DRS) as defined in HIPAA, regardless of whether your organization meets the definition of a covered entity or whether the electronic data is maintained using certified health technology. The following health information is excluded from the definition of EHI in the IB provisions: psychotherapy notes as defined in HIPAA, information compiled for a civil, criminal, or administrative action/proceeding, and electronic protected health information deidentified consistent with HIPAA.

You may be information blocking if you or your organization operationalizes any policies, processes, procedures, or workflows (i.e., practices) that you or your organization know (i.e., have requisite knowledge) are unreasonable and likely to interfere with the legally permissible access, exchange, or use of EHI and cannot meet the conditions of an allowable IB exception.

You can deny a request for access, exchange, or use of EHI, and this will not be treated as information blocking if you satisfy one or more of the IB exceptions provided in the rule by meeting all applicable requirements and conditions of the exception at all relevant times. There are eight IB exceptions:

1. [Preventing harm](https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-D/part-171/subpart-B/section-171.201),\* 2. [Privacy](https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-D/part-171/subpart-B/section-171.202),\* 3. [Security](https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-D/part-171/subpart-B/section-171.202), 4. [Infeasibility](https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-D/part-171/subpart-B/section-171.204),\* 5. [Health IT performance](https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-D/part-171/subpart-B/section-171.205), 6. [Content and manner](https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-D/part-171/subpart-C/section-171.301),\*   
7. [Fees](https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-D/part-171/subpart-C/section-171.302),\* and 8. [Licensing](https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-D/part-171/subpart-C/section-171.303).

The regulatory details of each exception are available by clicking on the exception. The asterisked exceptions are most relevant to the practices of individual providers or clinical staff and important for providers and the clinical staff to understand.

If your patient requests electronic access to their EHI, you must provide it in the electronic form (“manner requested”) and format requested if technically able to do so. You can offer to provide it in one of the alternate manners permitted in the IB Content and Manner exception if technically able and the patient agrees. Both the Cures Act and HIPAA rules apply to the patients’ right of access to their electronic records.

The Cures Act rule required EHR vendors with certified Health IT modules to comply with the [U.S. Core Data for Interoperability (V1)](https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi) standard for several certification criteria involving the sharing and exchange of health information, including transitions of care; clinical information reconciliation and incorporation; view, download, and transmit to 3rd party; transmission to public health agencies for electronic case reporting; application access–data request; and the standardized application programming interface (API) for patient and population services. This means individual providers should be able to, without any special effort or technical assistance, automatically or selectively push any of the clinical note types listed in the USCDI standard to the patient portal. Providers are required to share the following note types electronically with patients and other authorized requestors without delay unless they can meet and document an exception: consultation note, discharge summary note (not applicable to clinics), history & physical, procedure note, progress note (i.e., outpatient visit/encounter note), lab report narrative, pathology report narrative, and imaging narrative.

If your clinic uses the latest federally certified EHR technology, it should have native capabilities to share a patient’s records electronically, such as via the patient portal, secure messaging, or health information exchange for any or all of the data elements within the USCDIv1 data classes. This data should be readily available via the health IT module (usually the patient portal) certified to view, download, or transmit to a 3rd-party (VDT) criterion. This includes transmitting the data to a patient-facing application (“app”), such as a mobile health app, that conforms to the applicable application programming interface (API) standards and implementation guide for the certified API for patient and population services. The developer of a patient-facing app must register the app before it can connect to the certified EHR technology you use. The health IT vendor that provides your certified EHR technology should provide your organization with the details on their process for third-party app registration and tell your organization what you are required to do, if anything. If the patient-facing app was developed and implemented correctly and is able to successfully connect to your patient portal through your vendor’s certified API endpoint for patient and population services, the app must get the patient’s authorization for the app to receive some or all the patient’s EHI in the patient’s portal account before the app will be allowed to receive the data. Clinicians and their staff are not expected to know which patient-facing apps conform to the standards and can connect to their EHR system’s certified API endpoint for patient and population services. You should advise your patient to contact the app developer offering the app. Or alternatively, you could refer a patient’s question about whether a particular app can connect to your certified Health IT, to either your EHR vendor contact or your IT department depending on who provides your clinic’s IT support for your EHR. Clinicians and clinical operations staff should be familiar with the VDT functionality within the patient portal to inform or instruct patients or their authorized representatives.

Your patient has the right of access to all his/her EHI including mental health records, except psychotherapy notes and any EHI withheld to prevent harm to the patient or another person in accord with HIPAA harm standards. HIPAA does not provide special protection to mental health records in general (although your state law may), such as progress notes, but does give added protection to psychotherapy notes (i.e., “process notes”). Mental health professionals are permitted to share these notes with a patient if they choose to, but they are not part of a HIPAA DRS and are excluded from the definition of EHI. In accordance with the Cures Act rule, your EHR vendor must provide, by December 31, 2023, the capability to export a computable, machine-readable copy of all EHI for an individual patient or for all your patients. ONC did not require that this capability support a direct full EHI export by the patient. If your patient requests all the EHI in his or her electronic medical record beyond the USCDI data currently available to them through the patient portal, you may need to have your Health Information Management (HIM) or Information Services staff assist with fulfilling this request depending on your clinic’s HIM policies and procedures and technical capabilities. If your clinic does not have the technical capability to provide an EHI export to a patient or other authorized requestor, your clinic may meet the “Infeasible under the circumstances” condition under the Infeasibility exception but must respond in writing within 10 days of receipt of the request if it determines the request is infeasible under the circumstances.

For information about the data sharing capabilities of your technology or other related technical assistance, contact [include the contact info for the person that is the lead for providing this information and support to providers/clinical staff].

For questions on your clinic’s information blocking exception policies and procedures, contact [include the contact info for the person who the lead or authority on the information is blocking requirements and policies/processes for your clinic].

Attachment

Each of the examples below illustrate an IB exception scenario and the scenario assumes the provider or clinical staff have met all of the required conditions of the particular IB exception other than the one discussed in the example, including implementing the exception in a consistent and non-discriminatory manner and with required written organizational policies or a determination made in each case based on the particular facts and circumstances, and completing any required documentation and communications in the specified time period, as may be applicable.

Example 1: Preventing harm. You are a licensed medical practitioner and your minor patient’s father requests electronic access via his proxy access to his daughter’s patient portal account to the visit notes for a recent visit where you provided reproductive health services to the patient. As a matter of practice, you do not publish visit notes to the patient portal for certain reproductive health services for minors unless the patient agrees. You know the patient has a very volatile relationship with her father and is afraid of what her father might do if he knew about the details of the visit. You make an individualized determination using your professional judgement that your patient is at risk of substantial harm and have reasonable belief that withholding the information from the father will substantially reduce the risk of harm. You document this decision in writing in the patient’s chart and notify the father in writing you are not able to provide him with the information in order to respect your patient’s right to privacy. Note that the HIPAA substantial harm standard includes – physical, emotional, and psychological harm.

Example 2: Privacy – Precondition not satisfied. One of your patients in your multi-specialty practice moved out of the area and decided to see a provider near her new residence. All her records are electronic. The new provider, also in a multi-specialty practice, requests her entire electronic medical record including any behavioral health records since his clinic integrates behavioral health services within his practice. HIPAA does not require patient consent to share records for treatment purposes, but your state law does for behavioral health records, and your patient declines to provide her consent. You can decline to send the behavior health records and apply the IB Privacy sub-exception “Precondition not satisfied.” You document this in the patient’s chart. Your medical records staff transmits the other records right away since your clinic is still required under the IB provisions to share these without delay.

Example 3: Privacy – Respecting an individual’s request not to share. Your patient wants to give her husband proxy access to her patient portal account but does not want him to know she had an abortion prior to their marriage. If you are able to segment/restrict and flag this EHI as sensitive in your EHR system so it does not get published to the patient portal, you can meet the privacy sub-exception “Respecting an individual’s request not to share” and not share the information. If you are not able to segment this information electronically, you would need to advise your patient so she can decide whether she still wants to give her husband proxy access to her portal account.

Example 4: Privacy. Two of your clinic’s adult patients are siblings. One of the siblings had genetic testing and has a rare genetic disorder requiring treatment but has not shared this information with family members. It is possible the other sibling may have the same disorder and need treatment but has not had any testing done. The sibling with the disorder has requested that her diagnosis be kept private and requests that the information is not shared with her sibling. You are able to restrict this information in the EHR so it is not released to the other sibling or others without the patient's consent and explain to your patient why it would be important to consider sharing the information with her sibling. You would meet the privacy sub-exception “Respecting an individual’s request not to share” and possibly the sub-exception “Precondition not satisfied” if your state law prohibits disclosing genetic test results without patient consent.

Example 5: Infeasibility – Segmentation. Your state law allows minors to receive certain confidential services and providers may not disclose medical information or records about those services without the patient’s consent, even to the parents. The parent of one of your adolescent patient’s wants proxy access to her patient portal account; however, you do not have a way to technically segment the information the adolescent is able to keep private and wants to keep private from her parents. You can meet the infeasibility exception to deny electronic access by providing a written response to the parent’s request within 10 days of receiving the request to explain why it is infeasible to provide proxy access to the portal account. You also should inform the parent you can provide paper or PDF copies of the medical information you are permitted to share with the private information redacted but not electronically though the patient portal. You provide the parent a request form to fill out for your medical records staff to fulfill the request in accordance with HIPAA, including information on fees that would apply, if any.