

# Avoiding Information Blocking: A How-To Guide to Sharing Health Information Properly

## Quick Read Summary

You may have read articles and releases from other sources on the Cures Act. Here are three things to consider:

- Do not take the requirements under this act lightly, regardless of information you may have heard to the contrary. There are specific requirements of you as a provider. The law is real; it applies to you if you have electronic health information; and the information requests will come. Most of your healthcare colleagues in the allopathic medical community have an advantage – they have hospital system IT departments and compliance officers to take care of the details. Because chiropractic practices are typically smaller, most chiropractic physicians will have to handle the details themselves.
- Do not fear the Cures Act. Occasionally, you may receive correspondence about the Cures Act that attempts to scare you into action and possibly even overemphasize enforcement. Fear is not the best way to proceed into implementation of the Cures Act. The MCPA instead is providing factual information, including concrete steps for compliance to assist the typical chiropractic office with confident implementation of the new requirements.
- Understand that without the appropriate certified software (software that includes the “application programming interface,” or API, that complies with the Cures Act standards and allows different electronic records systems to easily transmit and receive information), you will be required to fulfill the requests with human intervention. It is possible to comply without certified software, but it will take more time. Also, there is a bonus to certified software – the Cures Act sets a deadline for when certified software will be required to allow for a full export of electronic health information. This will enable providers to be able to more easily change EHI systems if necessary.

Although all the details covered in this article are very important, and the MCPA urges you to review them in their entirety, at a minimum we strongly encourage you to know, read, and implement the following topics covered in sections below:

- 1) **The Cures Act DOES require healthcare providers to comply with the information blocking regulations** “regardless of whether any of the health IT the provider uses is certified under the ONC Health IT Certification Program.”<sup>1</sup>
- 2) You cannot charge patients fees for accessing or your time exporting and providing the requested information (i.e., these are free services you must perform for patients).
- 3) Read and understand the Privacy section.
- 4) Read and understand the Content and Manner section.
- 5) Read and implement the What to Do Now section.

---

As discussed at length in our previous articles, the 21st Century CURES Act is federal law that is designed to promote “innovation in the health care technology ecosystem to deliver better information, more conveniently, to patients and clinicians. It also promotes transparency, using modern computers,

smartphones, and software to provide opportunities for the American public to regain visibility in the services, quality, and costs of health care.”

In this article, the Missouri Chiropractic Physicians Association wants to help our doctors find the best method to adhere to the Cures Act regulations and requirements. Our previous articles covered the primary objectives of the interoperability portion of the Cures Act as they affect a chiropractic physician practice. You can access those articles here as follows:

- Overview,
- Interoperability (record sharing), and
- Information blocking.

Since the Cures Act law and regulations require that doctors share the records unless an exception applies, then compliance in everyday practice will often center around the exceptions. Below you will find explanations of the exceptions, when they may apply, required written policies for your practice, and how to implement the policies for each individual information request.

As a reminder, **the Cures Act DOES require healthcare providers to comply with the information blocking regulations**, “regardless of whether any of the health IT the provider uses is certified under the ONC Health IT Certification Program.”<sup>2</sup> Therefore, the general rule is that healthcare providers may not “information block,” even if they use uncertified EHI systems.

### When Can Providers NOT Give Access, Exchange, or Use of Information?

There are only five exceptions that allow providers to refuse to provide access in any form to electronic health information. These exceptions are: 1) preventing harm; 2) privacy; 3) security; 4) infeasibility; and 5) health IT performance. These are very nuanced and should not be used indiscriminately or *pro forma*. It is important to note that practices must develop written policies regarding how they will utilize the exceptions. Although there are three other “exceptions” to the information blocking prohibitions, they pertain only to HOW the requests are fulfilled. These last three “exceptions” still require providers to share ePHI but allow for some agreed modifications if applicable. All eight exceptions act as potential safe harbors for information blocking practices.

Following the exception explanations below, we will provide a step-by-step approach for practices to take to implement and adhere to the Cures requirements.

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

Preventing Harm Exception

Privacy Exception

Security Exception

Infeasibility Exception

Health IT Performance Exception

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

Content and Manner Exception

Fees Exception

Licensing Exception

## Privacy

In short, the Cures Act does NOT replace HIPAA. In fact, one of the major exceptions to the information blocking prohibition is to protect a patient's privacy. For example, if you receive a non-patient request for a specific patient's records or for a number of patient records, doctors should still ensure that their patients' privacy is protected. Details regarding HIPAA privacy are beyond the scope of this article,, but practices should ensure their HIPAA compliance manuals are up-to-date with policies that reflect the Cures Act requirements.

Remember, exercising the privacy exception is not to be used as just an easy way out. You must comply with a patient request for records quickly under both HIPAA and Cures. In fact, we anticipate that the Cures Act requests will come also as a HIPAA Right of Access request on behalf of the patient. This means that you must comply as soon as possible, but no later than 30 days. Note: New HIPAA rules have been released for comment that may potentially lower that timeframe to 15 days. We will notify members if and when that happens. For more information on right of access under HIPAA, see [this article](#).

Additionally, providers should update their HIPAA manuals AND Privacy Policies to reflect the Cures Act requirements. All requirements to provide written permission should be removed, as the ONC has determined that these types of requirements would be considered information blocking.

To summarize, if you receive a request from an app developer on behalf of the patient and you know that the request came from the patient, then the Privacy Exception does not apply.

## Security

As with privacy, the Cures Act does allow providers to block information (refuse to share) when a full risk analysis has determined that sharing the information would jeopardize the security of safeguarding the confidentiality, integrity, and availability of their stored electronic health information. Additionally, in order to use this exception, the reason for not sharing must be very specifically tailored to specific security risks and not because the provider "thinks" the practice is not secure. Lastly, the policy must be implemented in a consistent and non-discriminatory manner. In other words, a physician would not be able to determine that due to security concerns that he/she is not going to share information with any hospital system – there would have to be a specific security risk at stake.

All three of these elements (EHI is at risk, specific security issues, and non-discriminatory) must be met to use this exception. Providers should perform an updated HIPAA Security Risk Assessment, taking the Cures Act into consideration. ONC provides a toolkit for this assessment [here](#).

Some providers may have concerns about the security of the app that the patient has opted to use. The ONC sets aside this concern aside in their rules by stating, "An actor may not prevent an individual from deciding to provide its EHI to a technology developer or app, despite any risks noted regarding the app itself or the third-party developer."<sup>3</sup> In other words, providers may not use the security exception to refuse to provide a patient's EHI to a particular app simply because the provider deems it insecure.

For more information on having security "education" conversations with your patient, you can visit the [ONCs Patient Education and Engagement](#) page [here](#).

## Preventing Harm

Although this exception has the potential to be exercised more often with our colleagues in mental health and oncology than in the chiropractic profession, the ONC does want to protect “patients and other persons against unreasonable risks of harm.”**Error! Bookmark not defined.** This is one of the more discussed exceptions to information blocking in the mainstream healthcare world. In fact, there are hundreds of hours of podcasts, webinars, and attorneys’ articles to cover this issue. However, the ONC was very narrow when defining the requirements.

In short, this exception can only be used when a provider reasonably believes that by not releasing the requested information, there will be a substantial reduction to the risk of harm to an individual patient (or someone else). Additionally, they have clarified that “only danger to the individual’s ‘life or physical safety’ is recognized as grounds for denial of an individual’s right of access under” the Cures Act and this exception. That means providers can no longer hold test results because they may cause emotional challenges or because a patient may not be able to understand the raw results.

To exercise this exception, providers must make a professional judgement on a case-by-case, individual basis.<sup>4</sup> Blanket policies to withhold information are not allowed. [Click here](#) to review more information from the regulations regarding the preventing harm exception.

## Health IT Performance

This exception has a limited application and is only short term. It allows a delay when a health information technology system must be offline temporarily. These are rare occasions for maintenance or system degradation and must meet a specific set of criteria.**Error! Bookmark not defined.** We anticipate these cases will be very rare in a chiropractic office.

## Infeasibility

There are three things that would contribute to a provider NOT providing access to EHI under the infeasibility exception. Each can be considered separately:

- Uncontrollable Events – This would only apply during some level of emergency or disaster that would make it impossible for a provider to meet the request. For example, a hurricane damages a practice in Florida, and the doctor does not have access to the computer equipment to fulfil the request.
- Segmentation – This exception applies when the provider is not able to separate restricted information from the rest of the health information. The segmentation exception would impact those in the mental health field more often than chiropractic physicians. However, if a patient has requested that a portion of their medical record be restricted, and the provider cannot reasonably separate that portion from the rest, then the infeasibility exception can be exercised.
- Infeasibility under the circumstances – This exception is included in this category because it results in a complete denial of a records request. However, a provider may only use this exception **after the provider makes a good faith effort to comply using the “Content and Manner” method explained below**, which requires the provider to negotiate with the requestor to determine if the provider can share each portion of the information requested in a format that is acceptable to the requestor. The provider may only rely on the

“infeasibility under the circumstances” exception when the requestor does not accept the content and format offered by the provider. Therefore, it would not be possible for a provider to deny an information request “out of the gate” based on infeasibility without first attempting to come to an agreement with the requestor. More information on the Content and Manner exception will be covered below.<sup>5</sup>

If a provider uses any form of the Infeasibility Exception, then the provider 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 not possible. In other words, the provider has a shorter than the usual time frame of 30 days maximum. The Cures Act wants providers to act as soon as possible if they claim the exception that the request is infeasible.

### **The Exceptions Above Don’t Apply. How Do I Comply?**

The exceptions above, when properly met, all provide a safe harbor for providers to deny requested electronic health information. However, there are three other “exceptions” that are more procedures related to fulfilling information requests: Fees, Licensing, and Content and Manner.

#### **Fees**

The fees “exception” (albeit not really an exception) applies mainly to health information technology developers and how much they may charge electronic health information apps to connect to their system. However, this provision does not apply to provider and requests from patients.

“The rule includes a provision requiring that patients can electronically access all of their electronic health information (EHI), structured and/or unstructured, at no cost.” This is one of the key takeaways from the Cures Act and its rules. The fees “exception” specifically does not allow providers to charge patients for either access or exporting (i.e., downloading and sending).

#### **Licensing**

Like the Fees Exception above, this exception is designed for health IT developers and how they will be able to license apps to connect to their system. It has no effect on chiropractic physician practices.

### **Content and Manner (How Do I Comply?)**

The content and manner exception is the outlined procedure that will have the greatest impact on the chiropractic office. This procedure is designed to provide flexibility to providers concerning what information is required and how a provider should fulfill the request.

Perhaps the challenge that chiropractic physicians will most often face is that most chiropractic-centric EHR systems are no longer ONC certified and probably will not have the new application programming interface (API or how two applications/software communicate) that is required of certified EHI software for Cures. Since this technology will likely not be included in existing chiropractic office EHR information requests will require human intervention.

First, remember that the Cures Act requires that all electronic protected health information (ePHI) that a provider has must be shared when a request is received, unless an exception is met. ONC has

established a “phase in” timeframe for the extent of the data requirements, which is the “Content” portion of this exception/procedure:

**April 5, 2021** – All information included in the newly modified version 1 of the United States Core Data for Interoperability (USCDI V1) data set. The USCDI is a standardized set of health data classes and data elements for nationwide, interoperable health information exchange. Most of this information should be in a provider’s electronic health record system. To see the entire list, [click here](#).

**October 6, 2022** – All ePHI that you maintain is included. This will include all of the information that is required with the USCDI V1, plus information that may be stored in your practice/patient management software (i.e. all billing information, emergency contacts, future appointments, etc.).

This means that providers must provide the information included in the USCDI V1 dataset, *even if your system calls them something different* (for example, your system uses the term “Tobacco Use” instead of “Smoking Status” as referred to in USCDI V1).

Once a provider receives a request from a patient, you must determine if you can provide the information in the way (manner) requested. For example, the patient might ask you to send her records to her health records app she keeps on her mobile phone. If, as a provider, you are technically unable to provide the information in that way, then you must take the following steps without discriminating against the requestor or patient (only moving to the next step IF you cannot meet the current step):

- 1) Negotiate with the requester to find an agreeable format.
  - If no agreement -
- 2) Provide the information in a format available from certified software meeting ONC 2015 Standards (as of April 5, 2021) as requested by the requester.
  - If you cannot technically provide as in #2 -
- 3) Provide the information via “content and transport standards specified by the requestor and published by the Federal Government.”<sup>6</sup>
  - If you cannot technically provide as in #3 -
- 4) Provide the information via ANSI standards as specified by the requestor.
  - If you cannot technically provide as in #4 -
- 5) “Using an alternative machine-readable format, including the means to interpret the EHI, agreed upon with the requestor.”<sup>7</sup> This would typically be an XML file that looks similar to Figure 1.

```

<recordtarget>
  <patientRole>
    <id root="96A02DC3-C368-4773-BB43-84DBC3450FB6" extension="BeBo--19010101" assigningAuthorityName="Pay" />
    <addr use="HP">
      <streetAddressLine>123 street</streetAddressLine>
      <city>town</city>
      <state>AR</state>
      <postalCode>66666</postalCode>
      <country>US</country>
    </addr>
    <telecom use="WP" value="(345) 345-3453" />
    <patient>
      <name use="L">
        <given>Betty</given>
        <family>Boop</family>
      </name>
      <administrativeGenderCode codeSystem="2.16.840.1.113883.5.1" code="F" displayName="Female" />
      <birthTime value="19010101" />
      <ethnicGroupCode codeSystem="2.16.840.1.113883.6.238" codeSystemName="CDC - Race and Ethnicity" null />
      <languageCommunication>
        <languageCode />
      </languageCommunication>
    </patient>
    <providerOrganization>
      <id root="1.1.1.1.1.1.1.4" />
      <name>Spinal Health Chiropractic</name>
      <telecom use="WP" value="(123) 465-7890" />
      <addr use="WP">
        <streetAddressLine>2350 Huntington Dr

```

If after the negotiation and walking through each of these steps on a case-by-case basis the provider is unable to provide the data, then the provider can exercise the Infeasibility Under the Circumstances Exception. However, the provider must first walk through each of the steps above (including negotiation), document the results of each step, and then 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.

However, in advance of being able to exercise the Infeasibility Under the Circumstance Exception, providers must create a clear written policy that has taken into consideration the factors listed below and how the provider will apply these factors case-by-case:<sup>7</sup>

- The type of EHI and the purposes for which it may be needed;
- The cost to the actor of complying with the request in the manner requested;
- The financial and technical resources available to the actor;
- Whether the actor's practice is non-discriminatory and the actor provides the same access, exchange, or use of EHI to its companies or to its customers, suppliers, partners, and other persons with whom it has a business relationship;
- Whether the actor owns or has control over a predominant technology, platform, health information exchange, or health information network through which electronic health information is accessed or exchanged; and
- Why the actor was unable to provide access, exchange, or use of EHI consistent with the Content and Manner Exception in § 171.301.<sup>7</sup>

Remember that if you choose to use infeasibility, then you must respond in writing within 10 business days of receiving the request.

## What to Do Now

We understand that the information above and in our other articles may seem overwhelming or even over-informative. However, because of the case-by-case nature of many of the exceptions, the MCPA believes it is important to understand the concepts, along with the requirements. Below are some steps that practices should take to appropriately administer the new regulations and prevent information blocking.

- 1) Take an inventory of where all of your Electronic Health Information (EHI) is stored. Remember this would include your EHR system, appointment system if it contains ePHI, patient/practice management systems with ePHI, billing system, etc.
- 2) Look over the full list of required information in the [USCDI data set](#) (applicable between April 5, 2021 – October 5, 2022) to determine which system has the best data to share.
- 3) Once you have identified the system that has all of the required information (for now, that will probably be your EHR software), contact the vendor and ask the following questions:
  - a. Is the software currently certified by ONC?
  - b. Does it meet the new requirements for certification under the Cures Act, or will it meet them by April 5, 2021?
  - c. Does it have API built in or will it by April 5, 2021?
  - d. If the answer to b and c are yes, ask if they will provide training for those features.
  - e. If the answer is no to a, b, or c, ask if there is a way to download a patient's full file (with specified dates) in a computer readable format (typically XML).
- 4) Perform a HIPAA Security Risk Assessment, taking the Cures Act into consideration. ONC provides a toolkit for this assessment [here](#).
- 5) Update all relevant portions of your HIPAA manual AND your Privacy Policy to reflect the requirements under the Cures Act. Review the Privacy Exception above for more information.
  - a. Change any policies that require patients to request records in writing.
  - b. Update your Security section with any changes needed after your risk assessment is complete (see 4).
  - c. Remove references to charging patients for access to electronic health information. Remember, this does not necessarily apply to information requested other than electronic (i.e., paper copies). However, HIPAA Right of Access may apply when paper records are requested.
  - d. Verify that your Business Associate Agreements appropriately account for your new policies above.
- 6) Update any policies that would restrict access to test results (including x-rays and lab work) until after the doctor reviews the results. This practice would be considered information blocking.
- 7) Update any fee schedules that would charge patients for electronic health information. These types of requests must be **free for patients**. NOTE: this restriction would not apply to other entities such as insurance companies and possibly attorneys.
- 8) Create a policy that would consider each of the factors listed above under the Content and Manner exception. You should take into consideration the information you found in your inventory (1), data (2), and fact finding from your vendors (3).

Remember that although the new requirements will seem daunting and onerous, the purpose is to improve patients' understanding of their own health, placing them at the center and in control of their health information, easing access of ALL providers to ALL healthcare records, and improving outcomes. Additionally, the amount of data available will be an invaluable asset to the chiropractic profession and our ability to clearly demonstrate the efficacy of chiropractic patient-centered care, related to outcomes and cost effectiveness. Chiropractic physicians must be prepared to deliver according to the new standard of care and participate transparently with all other providers, health IT developers, health information exchanges, payors, and more.

---

<sup>1</sup> <https://www.healthit.gov/curesrule/resources/information-blocking-faqs>

<sup>2</sup> <https://www.healthit.gov/curesrule/resources/information-blocking-faqs>

<sup>3</sup> <https://www.federalregister.gov/documents/2020/05/01/2020-07419/21st-century-cures-act-interoperability-information-blocking-and-the-onc-health-it-certification>

<sup>4</sup> [https://www.ecfr.gov/cgi-bin/text-idx?SID=2469798090498a45fa9c432854f6196c&mc=true&node=se45.2.171\\_1201&rgn=div8](https://www.ecfr.gov/cgi-bin/text-idx?SID=2469798090498a45fa9c432854f6196c&mc=true&node=se45.2.171_1201&rgn=div8)

<sup>5</sup> <https://www.federalregister.gov/d/2020-07419/p-2498>

<sup>6</sup> <https://www.federalregister.gov/documents/2020/05/01/2020-07419/21st-century-cures-act-interoperability-information-blocking-and-the-onc-health-it-certification>

<sup>7</sup> <https://www.healthit.gov/condition-ccg/information-blocking>