Davis Brown Health Law Blog

Information Blocking: Compliance Regulations Pushed Back to Spring 2021 – November 25, 2020

Jo Ellen Whitney

Recognizing the difficulty of managing interoperable technology as well as the pressures from the global pandemic, the Department of Health and Human Services (HHS) announced a delayed implementation of the Cures Act, Section 4004.

Section 4004 includes information blocking rules, regulations intended to provide patients easy access to their records and help facilities share patient information, with the goal of ultimately providing better healthcare.

The information blocking rules in the Cures Act were scheduled for an initial implementation and enforcement date of November 20, 2020. On October 29, 2020, HHS announced that implementation would be pushed to April 5, 2021.

Given that we now all have a little extra time to think, or worry, about this, it is worth reassessing what Section 4004 is intended to do.

Information Blocking Regulation Intent

The intent of the regulations is to remove barriers to patient access to healthcare and improve interoperability between systems with the goal of better individual and population health. The regulations include all software that create, track, or store electronic patient data, so not just the standard EMR, but also the auxiliary systems which feed into an EMR or other places as well.

HHS and the Office of the National Coordinator (ONC) indicated that this is in line with its mission as set forth in the Patient Access Initiative and that it is intended not only to promote patient access but to limit any competitive behaviors that hinder the exchange of medical information.

Information blocking, as prohibited by the statute, is considered to be any process that is likely to interfere with access to and reasonable use of Health IT. In essence, ONC summarizes this as “nonstandard” processes which make access more complicated, slower, or which would prevent access in circumstances that are not required by other laws such as HIPAA.

The ONC is charged with enforcing the Cures Act and has issued the primary implementing regulations. There are a variety of requirements including the development of apps so patients can access their medical records from mobile devices, interoperability standards as well as the revision of internal facility policies in hospitals, clinics, and other places where EMR's are used to promote consistent patient access and continuity of care. This ultimately is also likely to relate to the use and sharing of social determinate information (SDI) which has been in something of a gray area in regard to HIPAA and its potential request for use by social service agencies and law enforcement.

Interoperability

HHS and ONC have the intent to encourage interoperability. When we think of interoperability, we frequently think of access between our own hospital or clinic and someone else's hospital. It is important to know that interoperability also impacts a number of other areas relating exclusively to internal systems.

The number of devices healthcare providers use internally daily that capture data is staggering. Some systems are designed to limit data transfer to other systems or equipment, which can be a problem when a hospital attempts to change vendors later. These vendor contracts prevent the hospital from migrating legacy data. The interoperability rules are intended to mitigate that effect, which in the long term can be a substantive benefit to hospitals, clinics, and others who enter into vendor contracts giving these providers greater choice and flexibility.

Easy access between systems can also improve patient outcome and choice by fostering seamless continuity of care, while requiring the development of endpoints for mobile devices increases access for many who do all of their online access from a phone.

Things to Resolve

The rules have also created some concerns which, even with clarification from ONC, will require time to assess, answer, and resolve.

1. What do we do about minor access to portals?

It has always been difficult in Iowa to determine when parental access to a minor's portal should be cut off. Because Iowa has no single date of emancipation for minors other than the age of 18, when they are considered adults, it can be difficult to determine what information a parent may or may not access. Minors can consent to certain forms of treatment, such as STI/STD testing, while they can't consent to the setting of a broken arm. Because of this, many systems have chosen what they consider to be reasonable dates to cut off parental access to portals with typical ages being 12, 13, and 14.

However, under the information blocking rules, blocking access to a minor's portal at age 12, or even 14, could be considered a violation of the rules as it would impede access of the parent to information he or she is allowed to access by law. This can create substantive issues in trying to manage access to minor's medical information as many existing EMR systems do not allow segregation of certain data (such as STI/STD test results) from the general records. Another solution some facilities have used, simply not having portals for minor's records, runs contrary to the standards relating to portals and information blocking expectations.

This is an area that facilities need to address in their internal policies and Notice of Privacy Practices as well as through programming with their EMR and other software providers.

2. Delaying test results

Some facilities choose to delay posting test results until a physician or other health care provider has had the opportunity to speak with the patient regarding those results. Delaying test results in this manner is likely to be considered a violation of the information blocking regulations. The anticipated rules have already resulted in many facilities posting test results to a portal at the same time that they are provided to the ordering physician. It is clear that this can sometimes be upsetting for patients, particularly if they required complex testing or had an unfavorable outcome.

Patients will need additional education to address this rapid test result access and facilities will need to be particularly diligent in contacting patients when they call with questions about test results they've already seen. Staff training will also be needed to properly address patient concerns.

3. Provider created restrictions

While it is uncommon in Iowa, some providers nationally have created individualized restrictions for the release of records for a variety of reasons specific to the facility or provider. Individual restrictions of this type, which are not based on clear regulatory guidelines, are unlikely to have been a good idea prior to the information blocking regulations but certainly run afoul of the new regulations.

In September 2020, the Office of Civil Rights (OCR), the companion agency to ONC, issued five fines and citations to providers for failure to allow patient access. At least of some these clearly related to individualized provider restrictions which were not otherwise allowable under HIPAA.

4. The role of third-party records

Third-party records have always occupied a complicated space for many facilities who may rely on the records but aren't certain whether they should be produced pursuant to a patient request. The fundamental concern for most facilities has been whether the records are accurate or complete and the fact that we do not want patients to rely on a record that was not created by our facility. Essentially, a standard liability concern.

Under HIPAA, the rule has traditionally been that if you accept the records, if they are scanned into your EMR system, and you use those records or rely on them, they become part of your Designated Record Set. They are then subject to production upon a request for records. Many facilities that use this process, provide a disclaimer as part of the record production stating that the record may include records from third parties and that the facility cannot attest to the truth, veracity, or completeness of these third-party records.

Other facilities, such as teaching hospitals that may receive an extraordinarily large amount of records from other providers due to the complex nature of cases that come to them, may choose not to accept records, not to keep the records, or to segregate them in a separate system to avoid creating an expectation that they would be part of the Designated Records Set. It is not clear how this process will work under the information blocking regulations, but a likely outcome is that the information received from third parties will be incorporated into the record set, which can then be subpoenaed or requested for release. These are policy issues that need to be addressed internally so that you can be efficient and consistent in processes.

5. Transfer outcomes

Many hospitals and facilities such as long-term care centers may transfer patients for emergencies, specialty care, and other reasons. Many EMR systems have developed interoperability if these facilities are using the same vendors so the transferring facility can review documentation from the new facility to determine how the patient has progressed and if the care received at the original facility was appropriate.

This is another murky area where facilities need additional information to understand how that type of review will be treated under the information blocking regulations. While it can be argued that evaluating information from another facility is part of the continuity of care process or falls under the operations exemption of HIPAA, some facilities have treated it as an inappropriate review of information either for competitive purposes or stated simply that it exceeds the HIPPA minimum necessary expectations for transfer of data.

Since HIPAA is a rule of notice, there are various ways to address this. This may include clear statements in your NPP for patients and clear expectations set amongst various facilities so that all parties are aware that operational and continuity of care data access may occur.

Under the OCR and ONC rules, as well as just generally, you can almost never go wrong with being transparent in what data you will access and review. It should be noted that the information blocking regulations do not change the fundamental privacy practices of HIPAA or higher levels of privacy which are provided by state law for things such as mental health treatment and HIV/AIDS.

Exceptions

In its final rule, ONC delineates eight exceptions to the information blocking rule divided into two classes:

Class 1: Exceptions that involve *not* providing information

1. Preventing harm

Preventing harm is essentially the Tarasoff standard which is also incorporated into Iowa Code 229. This provides that information may be withheld if there is a reasonable belief that this will substantially, “reduce the risk of harm,” that the practice is compliant with the minimum necessary limitations, and that any policy assesses risk, type of harm, and implementation. The patient has the right to request an individualized determination of the risk of harm. Records which do fall into the risk category may not be withheld. This is likely to be most pertinent in mental health and similar records situations where the release of certain information could cause self-harm or harm to others. Any utilization of this provision or policy involving this exception should consider the existing Iowa statutes regarding these matters.

2. Privacy

As noted above, the rules recognize that the HIPAA privacy requirements are not waived by this new regulation. This section recognizes that all of the general HIPAA and state-based exceptions apply. This includes the patient’s right to choose not to share information with an insurance company when the patient pays for his or her own care and also provides an exception for Health IT developers of technology who are not otherwise covered by HIPAA.

3. Security exception

This covers all basic security processes related to firewalls and other security implementation. Requiring identifiers or passwords is not considered to be a violation of the information blocking rules. So long as the processes are "implemented in a consistent and nondiscriminatory manner."

4. Infeasibility

Or if it's just not possible, the "infeasibility exception." The regulations recognize that there are some instances where it is simply not possible to provide access to information. This may involve uncontrollable events, such as when the entire county has been hit by a tornado, there is a public health emergency, or public safety incident. Note: *you must provide a written response to the person requesting the records within 10 business days of receipt of the request as to the reasons why the request is not feasible.*

5. **Health IT performance exception or timeout for maintenance**

The rules recognize that information may be temporarily unavailable due to maintenance, repairing a firewall, or something similar. We can infer from this that if your facility or system is under attack via ransomware, you may not be able to provide the information, although you may have reporting and other HIPAA issues to deal with.

Note that if this maintenance is intended to slow down or block access to information or is a "nonstandard" process it will be subject to enforcement action. You can't conveniently be doing system updates to get around a subpoena.

Class 2: Exceptions that involve *how* you provide information.

1. Content and manner exception

This notes that certain data may potentially be excluded. A common state law exception would be peer review data as well as psychotherapy notes, and information compiled in a reasonable anticipation of or for use in a civil, criminal or administrative action or proceeding. It also allows facilities to provide information in alternative formats if you are technically unable to meet the production requirements in the requested format.

Note that HIPAA does require that you provide documentation in an electronic format where requested by a patient or patient representative. There are some sliding deadlines for access specifically referenced in the rules.

2. Fee exceptions

The intent of the rule is to make patient access to healthcare information cheap and fast. The rules here are similar to those previously set forth in the Patient Access Initiative and OCR guidance, including the statement that all fees charged must be "reasonably related to the provider's cost, providing the type of access, exchange or use of the EHI." Remember that OCR is hoping that records will be made available electronically for a cost of no greater than $6.50, although certain exceptions to this expectation apply.

3. Licensing exception

This exception allows vendors and others to charge reasonable royalties in order to "protect their innovations." If there is no existing license through preexisting contracts the rule provides that, "a provider 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 Big Picture

For the last several years, OCR and ONC have been working together on patient access issues. This year, OCR has issued several corrective action plans and corresponding fines, ranging from $3,500-$160,000 - all relating to the release, or lack thereof, of patient records. This follows a number of other similar violations cited by OCR.

Taken in conjunction with the information blocking regulations drafted and administered by ONC, this indicates that HHS is extremely serious about patient access. So, as if there isn't enough to think or worry about during a pandemic, healthcare facilities need to work with their legal counsel to create a plan that addresses all of the areas above and then some.
