BLOCKING AND TACKLING: WHAT EVERY HEALTH CARE PROVIDER'S LEGAL, IT, AND COMPLIANCE TEAMS NEED TO KNOW ABOUT INFORMATION BLOCKING TO MAKE IT THROUGH THE FIRST COMPLIANCE DEADLINE'S GOAL POSTS

Date: 1 October 2020

Health Care Alert

INTRODUCTION

The Department of Health and Human Services' Office of the National Coordinator for Health Information Technology (ONC) is responsible for the implementation of key provisions of Title IV of the 21st Century Cures Act (Cures Act), which are designed to advance interoperability of health information; support the access, exchange, and use of electronic health information (EHI); and address occurrences of "information blocking" of EHI.[1] On 1 May 2020, ONC published its much anticipated Final Rule on Interoperability, Information Blocking, and the ONC Health IT Certification Program (the Final Rule).[2] With the initial Information Blocking compliance deadline of 2 November 2020, approaching, health care providers are quickly learning that tackling the Final Rule's new requirements will require a team effort and a well-planned strategy.[3]

The Final Rule implements two key provisions of the Cures Act: (1) Conditions and Maintenance of Certification requirements for health information technology (health IT) developers, including the voluntary certification of health IT for use by pediatric health providers; and (2) identification of reasonable and necessary activities that do not constitute "information blocking." These portions of the Cures Act, which the Final Rule implements, in essence require providing patient access to EHI in a form convenient for the patient, such as improving the electronic accessibility of a patient's EHI through the adoption of standards and certification criteria and the implementation of information blocking policies that support patient electronic access to their EHI at no cost. As stated by ONC Deputy Director Steven Posnack during an ONC-sponsored webinar, "In its entirety, the Rule covers a wide range of intersecting health and health IT policy issues, but at its heart, it focuses on giving patients the ability to access their data, improve the ability for health care providers to deliver care, and promote competition."[4]

In addition to fulfilling the Cures Act's requirements, the Final Rule contributes to fulfilling Executive Order (E.O.) 13813, issued 12 October 2017. The E.O. is intended to promote health care choice and competition across the United States, emphasizing that government rules affecting the U.S. health care system should re-inject competition into health care markets by lowering barriers to entry and preventing abuses of market power. The E.O. also states that government rules should improve access to and the quality of information that Americans need to make informed health care decisions. As an example of how the Final Rule contributes to the E.O.'s

©2005-2026 K&L Gates LLP. All Rights Reserved.

objectives, it establishes application programming interface (API) requirements, including those that require providing patients access to their EHI "without special effort," as well as supporting health care providers' independence to choose the "provider-facing" third-party services of their choice to interact with the certified API technology they have acquired.

The Final Rule was codified in the Code of Federal Regulations on 30 June 2020, at 45 C.F.R. Parts 170 and 171. While the Final Rule contains many important provisions, the Information Blocking Rule is a key component. With the first Information Blocking compliance deadline of 2 November 2020, approaching, health care providers are organizing internal stakeholders to consider what policies and procedures and applicable IT solutions they will have to implement. While the overarching purpose and intent of the Information Blocking Rule is clear, many aspects of the Final Rule require a facts and circumstances analysis, including what practices may be considered information blocking, what constitutes a delay in providing access, and when health care providers may also be considered "Health IT Developers" and "HIEs/HINs" (both defined below). This leaves health care providers' IT, Health Information Management, Compliance, and Legal Departments navigating the nuances of a 322-page Final Rule for additional guidance and clarity. We have provided guidance to many of these entities on a multitude of issues, and have outlined some of the more pressing issues in this alert.[5]

WHAT IS INFORMATION BLOCKING?

The Information Blocking Rule governs three categories of actors: developers of certified health IT (Health IT Developers), Health Information Exchanges and Health Information Networks (HIEs/HINs), and Health Care Providers, collectively referred to in the Information Blocking Rule as "actors."[6] A practice may be considered "information blocking" under the Information Blocking Rule if it is likely to interfere with access, exchange, or use of EHI, and if it meets the applicable standard, depending on the actor. Practices of Health IT Developers and HIEs/HINs will be information blocking if the actor knows, or should know, that such practice is likely to interfere with access, exchange, or use of EHI. Practices conducted by a Health Care Provider may be considered information blocking if the Health Care Provider knows that such practice is unreasonable and is likely to interfere with the access, exchange, or use of EHI.[7]

For purposes of the Information Blocking Rule, the phrase "interfere with" means to prevent, materially discourage, or otherwise inhibit.[8] Some examples from the proposed rule and Final Rule of practices that may "interfere with" access, exchange, or use of EHI include, but are not limited to, the following:[9]

- Formally restricting access, exchange, or use of EHI, such as through contractual terms, EHI sharing policies, or organizational policies or procedures, for example a health system's internal policies or procedures that require staff to obtain an individual's written consent before sharing the patient's EHI with unaffiliated providers for treatment purposes, even though obtaining such consent is not required by state or federal law;
- Unnecessarily slowing or delaying access, exchange, or use of EHI, or otherwise limiting the timeliness of EHI accessed or exchanged; and
- Charging an individual, their personal representative, or another person or entity designated by the individual for electronic access to the individual's EHI.

©2005-2026 K&L Gates LLP. All Rights Reserved.

ONC reiterated that its list of examples that may interfere with access, exchange, or use of EHI is not meant to be exhaustive, and "any conclusions regarding such interference would be based on fact-finding specific to each case and would need to consider the applicability of the exceptions."[10] In fact, a practice is not information blocking if (a) the practice is required by law (e.g., federal regulations that prevent the disclosure of substance use disorder records), or (b) the practice is covered by one of eight exceptions promulgated by ONC.[11]

While ONC states in the Final Rule that the information blocking provision would be implicated if an actor were to engage in "exclusionary, discriminatory, or other practices that impede the development, dissemination, or use of interoperable technologies and services that enhance access, exchange, or use of EHI,"[12] not all instances of differential treatment necessarily constitute a discriminatory practice that implicates the information blocking provision. For example, different fee structures or other terms tied to the access and use of EHI may reflect legitimate differences in the cost, quality, or value of the EHI and the effort required to provide access, exchange, or use.[13]

EXCEPTIONS TO INFORMATION BLOCKING

In the Information Blocking Rule, ONC developed eight exceptions, each of which recognizes important objectives that merit practices that might otherwise be considered information blocking. Exceptions are divided into two categories: (1) exceptions that involve not fulfilling requests to access, exchange, or use EHI; and (2) exceptions that involve implementing procedures for fulfilling requests to access, exchange, or use EHI. To meet any exception under the Information Blocking Rule, the actor must meet all applicable requirements and conditions of the exception at all relevant times.

A high-level summary of each of the eight exceptions to the Information Blocking Rule is outlined below. It is important to note that each exception contains specific conditions that must be met, so it will be important for actors to fully understand the implications of these exceptions.

Provided certain conditions are met, it will not be information blocking for an actor to interfere with access, exchange, or use of EHI for the following reasons:

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

- Preventing Harm: Where the practice is reasonable and necessary to prevent harm to a patient or another person[14]
- Privacy: To protect an individual's privacy[15]
- Security: To protect the security of EHI[16]
- Infeasibility: Where it is infeasible to fulfill the request[17]
- Health IT Performance: Where the practice is a reasonable and necessary measure to make health IT temporarily unavailable or to degrade the health IT's performance for the benefit of the overall performance of the health IT[18]

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

©2005-2026 K&L Gates LLP. All Rights Reserved.

- Content and Manner Exception: Where the practice limits the content of the response to a request or the manner in which the actor fulfills such request[19]
- Fees Exception: Where an actor charges fees, including fees that result in a reasonable profit margin[20]
- Licensing Exception: Where an actor licenses interoperability elements for EHI to be accessed, exchanged, or used[21]

Even if a practice implicates the information blocking prohibition but does not meet an exception, the practice may nevertheless not actually constitute impermissible information blocking. ONC states that "to implicate the provision is not necessarily to violate it, and … each case will turn on its own unique facts."[22] In any particular case, ONC will utilize a facts and circumstances analysis to determine if information blocking has occurred. In particular, ONC states that "[a] practice failing to meet all conditions of an exception only means that the practice would not have guaranteed protection from civil monetary penalties (CMPs) or appropriate disincentives. The practice would instead be evaluated on a case-by-case basis to assess the specific facts and circumstances (e.g., whether the practice would be considered to rise to the level of an interference, and whether the actor acted with the requisite intent) to determine whether information blocking has occurred."[23]

HEALTH CARE PROVIDER FREQUENTLY ASKED QUESTIONS

The Final Rule established several important time periods and compliance deadlines, the first of which is 2 November 2020. The first six months after publication of the Final Rule, from 1 May 2020, through 1 November 2020, is a preparation period, during which compliance is encouraged.[24] Beginning six months after publication of the Final Rule – 2 November 2020 – actors must comply with the Information Blocking Rule by providing EHI that consists of, at a minimum, United States Core Data for Interoperability (USCDI) data elements, which are a discrete set of EHI data elements[25] described in detail on ONC's website. As Health Care Providers prepare for this first compliance deadline, they are seeking guidance on a number of common issues, some of which we have cataloged here. Considering the number of nuanced issues related to the Information Blocking provision, including understanding and applying the exceptions, we will continue to provide additional guidance through future alerts and episodes of our podcast, *Triage*.

Among the points of most concern to Health Care Providers as they prepare for compliance with the Final Rule, are (a) whether and to what extent the Information Blocking Rule will apply to different practices, (b) what types of data are subject to disclosure under the Information Blocking rule, and (c) what penalties may apply for a violation of the Information Blocking Rule. We have provided responses below to several of these specific issues and questions. While compliance with the Final Rule and analysis of whether a particular practice would be considered Information Blocking requires a fact-specific inquiry, a general understanding of ONC's approach to the implementation of the Final Rule in key areas is helpful to informing Health Care Providers' decision making as they prepare for the upcoming compliance deadline.

©2005-2026 K&L Gates LLP. All Rights Reserved.

ARE HEALTH CARE PROVIDERS REQUIRED TO COMPLY WITH THE INFORMATION BLOCKING RULE EVEN IF THEY DO NOT HAVE CERTIFIED HEALTH INFORMATION TECHNOLOGY?

The Cures Act does not prescribe that only practices involving technology certified by ONC's Health IT Certification Program implicate the Information Blocking provision. Thus, "actors" as defined by the Information Blocking Rule, including Health Care Providers, are required to meet the information blocking requirements with regard to EHI, regardless of whether such EHI is through the use of technology certified under ONC's Health IT Certification Program. Accordingly, Health Care Providers cannot engage in practices that constitute information blocking in relation to EHI, and these entities should avoid practices that "are likely to interfere with access, exchange, or use of EHI," where they have knowledge that such practice is unreasonable and likely to interfere with access, exchange, or use of EHI.[26] As reiterated by ONC, it is important to note that, for an individual or entity to meet the definition of Health IT Developer of certified health IT, they must have had, at the time of the practice in question, one or more health IT modules certified under the ONC's Health IT Certification Program, so there is a connection for Health IT developers of certified Health IT to ONC's Health IT Certification Program.

HOW IS ELECTRONIC HEALTH INFORMATION (EHI) DEFINED?

The Final Rule modifies the 2015 Edition health IT certification criteria and ONC Health IT Certification Program in ways that, in ONC's opinion, will advance interoperability, enhance health IT certification, and reduce burden and costs. A portion of the 2015 Edition called the Common Clinical Data Set (CCDS) has been replaced with the USCDI (United States Core Data for Interoperability), which include a discrete set of standard EHI elements described in detail on ONC's website.[27] This means that certain data classes and data elements for certified health IT, including EHRs, are changing. Relevant to this discussion, USCDI adds the following data elements and standards that were not included in the previous version of the 2015 Edition: (1) clinical notes; (2) provenance data; and (3) better demographics for patient matching. While health IT developers will not be required to meet the 2015 Edition certification criteria until 18 months from the first compliance deadline of 2 November 2020, the Information Blocking Rule indicates that "EHI," for purposes of Information Blocking, is limited to the EHI identified by the data elements represented in the USCDI standard, beginning 2 November 2020. This means that the USCDI data elements outline the list of data that is required to be disclosed to avoid a claim of Information Blocking, but USCDI's data standards and code sets are not required for certified health IT until May of 2022.

After 2 May 2022, "EHI" for purposes of Information Blocking will include electronic PHI in a Designated Record Set, as those terms of defined by HIPAA's Privacy Rule.[28] That date also coincides with the deadlines for developers to certify that certified EHR and other health IT meet the USCDI data elements, standards, and code sets.

In explaining that it would define "EHI" for purposes of Information Blocking for the first eighteen months as the USCDI data elements only, as opposed to the full EHI definition of ePHI in a Designated Record Set (DRS), ONC commented as follows:

©2005-2026 K&L Gates LLP. All Rights Reserved.

> By using USCDI as the baseline of EHI for 18 months after the compliance date of the information blocking section of this final rule (45 CFR part 171), we have created a transparent, predictable starting point for sharing the types of EHI that is understood by the regulated community and more readily available for access, exchange, and use. In addition, health IT that has been certified to the 2015 Edition ''CCDS'' certification criteria will be able to immediately and readily produce almost all of the data elements identified in the USCDI. Furthermore, most, if not all, of such health IT already supports recording USCDI data elements and most HIEs/HINs are routinely exchanging such data elements.[29]

RELEASE OF LEGACY, OR HISTORICAL, DATA, INCLUDING CLINICAL NOTES

The Information Blocking Rule at Part 171 of the regulations requires that EHI, as defined by the regulations, that exists at the time of a request and is controlled by the actor, be made available for access, use, or exchange, subject to practices that otherwise interfere with access, use, or exchange that are required by law or are pursuant to an Information Blocking exception. The focus of Information Blocking is to enable access, use, or exchange of EHI that exists and is controlled by the actor, and neither the Commentary nor the regulations specifically address historical data; rather, if the information exists, an actor must provide it pursuant to a request, in the manner requested. As stated above, the Final Rule modifies the 2015 Edition health IT certification criteria and ONC Health IT Certification Program such that the CCDS has been replaced with the USCDI, and EHI, for purposes of Information Blocking, includes the new USCDI data elements beginning November 02, 2020. To the extent an "actor" subject to the Information Blocking Rule has "EHI," as defined by the regulation, within its control at the time of a request, it should provide that data in the form requested, unless as stated above, an exception applies to either the data, or the manner in which the data can be provided, or both. In particular with regard to the new USCDI data elements that were not previously available under the CCDS standard, the Content and Manner Exception may be applicable.[30]

DELAYING RELEASE OF TEST RESULTS AND THE PREVENTING HARM EXCEPTION

Pursuant to the Information Blocking Rule, information required to be accessible to the patient should be available without delay, though what constitutes "without delay" will be dictated by the type of record and the request. In commentary related to what is considered "timely" access to EHI, ONC commented that it has not established a timeframe, given the tremendous variability in terms of the scope of health IT. Accordingly, "timely access" will be a facts and circumstances analysis. It is illustrative that, within those same comments, ONC refers to its commentary on limiting or restricting the interoperability of EHI, specifically its admonishment that "slowing or delaying access, exchange, or use of EHI could be considered information blocking." Like its approach with what constitutes "timely" access, ONC indicates that "unnecessary delays or response times" that otherwise limit the timeliness of EHI may be considered information blocking, depending on the facts and circumstances.

We advise clients to consider this issue within the context of the Information Blocking Rule, which seeks to remove unnecessary impediments or obstacles to complete interoperability, including many of the protective measures health care providers traditionally have taken on behalf of the patient. ONC also provides many clues

©2005-2026 K&L Gates LLP. All Rights Reserved.

regarding the types of delays that would be considered information blocking, such as delays that allow providers to maintain control over communications of test results but do not otherwise meet the Preventing Harm Exception. From this, and in the absence of a defined term, we can begin to understand the way ONC will analyze what constitutes "timely" and what would be a "delay."

For example, many Health Care Providers delay the release of lab records in an attempt to protect patients from misinterpreting results, or from learning about potentially life-altering results without the guidance and perspective of their practitioner. Even where the intent of a particular practice that interferes with the access, exchange, or use of EHI is in the patient's best interest, such practice may be information blocking, unless the practice is required by law or covered by an exception. The applicable exception to a delay in the release of test results for the purpose of facilitating communication between the patient and the Health Care Provider is the Preventing Harm Exception; however, ONC in commentary to the Final Rule specifically stated that "routinely time-delaying the availability of broad classes of EHI will not fall under the Preventing Harm Exception."[31]

ONC further stated that it saw no evidence that a routine delay intended to foster the clinician-patient relationship would substantially reduce danger to life or physical safety of patients or other persons. Rather, any determination to delay lab results, unless required by law, would need to be based on "specific circumstances" where providers retaining full control over communications are "reasonable and necessary" to substantially reduce a risk of harm cognizable under the Preventing Harm Exception, as determined on a case-by-case basis or due to circumstances where the data is known or reasonably suspected to be misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason.[32] Accordingly, in developing policies related to the release of test results, Health Care Providers should clearly outline the Preventing Harm Exception and educate its workforce on its application on an individualized basis.

RECORDS SUBJECT TO FEDERAL OR STATE LAWS WITH HEIGHTENED DISCLOSURE REQUIREMENTS

Information blocking specifically excludes practices that interfere with the release of EHI that are required by state or federal law; therefore, such practices would not violate the Information Blocking Rule.[33] However, when a law prohibits the release of only certain information, the Information Blocking Rule will apply to that portion of the record that is not protected by law, and an exception must be met before restricting access to the rest of the record. For instance, many states' laws related to the treatment of minors allow minors to consent, without requiring a court order or any other adult consent, to the provision of health care for certain health conditions, such as pregnancy, sexually infectious diseases, and substance use disorders. In those situations, the Privacy Rule under the Health Insurance Portability and Accountability Act (HIPAA) allows for the minor to control the release of such records (with some exceptions and subject to state laws that specifically address access); however, typically the minor would not control release of his or her entire medical record. Similarly, a federal law at 42 C.F.R. Part 2, commonly known as "Part 2," provides for heightened protection related to the release of substance use disorder records that would identify an individual as having or having had a substance use disorder and obtained by certain "Part 2 Programs." In each of these instances, the law at issue generally would not apply to the entirety of the patient's medical record. Accordingly, actors would need to segment records that are otherwise part of a Designated Record Set (as defined by the Final Rule with reference to HIPAA's Privacy

©2005-2026 K&L Gates LLP. All Rights Reserved.

Rule), but are not covered by a federal or state law, as such records would be subject to the Information Blocking Rule, unless an exception applies.

PENALTIES

The 21st Century Cures Act prescribes penalties for information blocking. Health IT Developers and HIEs/HINs are subject to CMPs of up to one million dollars per violation. Health Care Providers, however, are not subject to CMPs; rather, they will be subject to "appropriate disincentives."[34] CMPs will not be enforced against Health IT Developers and HIEs/HINs until such CMPs are established through notice and comment rulemaking by the United States Department of Health and Human Services' Office of Inspector General (OIG).[35] ONC published a proposed rule addressing CMPs on 24 April 2020.[36] The rule has not yet been finalized, but the comment period closed 23 June 2020.

COMPLIANCE DEADLINES AND NEXT STEPS

Compliance with the Information Blocking Rule will occur in three phases:[37]

1. The first six months after publication of the Final Rule is a preparation period, during which compliance is encouraged (1 May – 2 November 2020).
2. Beginning six months after publication of the Final Rule (2 November 2020), actors must comply with the Information Blocking Rule, but are governed by a limited definition of "EHI," such that responses to requests may be limited to the data elements represented in the current USCDI standards.
3. From month 24 onward after publication of the Final Rule (2 May 2022), actors must comply with the Information Blocking Rule, and responses to requests to access, exchange, or use EHI must include the full scope of EHI, as defined at 45 C.F.R. § 171.102.

CONCLUSION

While much remains to be seen with regard to ONC's enforcement of the new requirements under the Final Rule once it takes effect, the volume and tone of commentary and guidance offered by ONC indicate that the Final Rule, and the Information Blocking Rule in particular, are intended to represent a sea-change in the movement and availability of health care data. Accordingly, it is important for actors to carefully consider whether short and long-term adjustments to their day-to-day operations are required, including the development of policies and procedures that are beneficial to both patient and Provider, as well as compliant with each phase of Information Blocking compliance.

As the first compliance date approaches, we will continue to monitor for updates to ONC guidance related to implementation and enforcement of the Final Rule, and will further report on ONC and OIG enforcement policies and promulgation of a Final Rule related to penalties, including CMPs and disincentives.

For assistance in further understanding the intricacies of the Final Rule, or in developing policies and procedures to assure compliance, contact K&L Gates through the contacts in this alert.

©2005-2026 K&L Gates LLP. All Rights Reserved.

FOOTNOTES

[1] In response to Congress passing the 21st Century Rules Act in December of 2016, ONC met with stakeholders affected by health information interoperability and information blocking and consulted with several federal agencies, including the Department of Health and Human Services' Office of Inspector General and Office for Civil Rights and the Federal Trade Commission. On March 04, 2019, ONC issued its Proposed Rule and received over 2000 comments submissions.

[2] The full text of the ONC Final Rule on information blocking is available here.

[3] While ONC has indicated that, due to the COVID-19 national pandemic, it will exercise discretion in enforcing key components of the ONC Health IT Certification Program, codified at 45 C.F.R. Part 170, until three months after each initial compliance date or timeline as outlined in the Final Rule, it has not extended compliance deadlines for the Information Blocking Rule at 45 C.F.R. Part 171.

[4] *See ONC, ONC's Cures Act Final Rule Webinar - Overview, April 24, 2020*, located here (visited August 30, 2020).

[5] While additional components of ONC's Final Rule merit further consideration, for purposes of this alert, we will focus on key aspects of the Information Blocking Rule, and we will address additional components of the Final Rule in future alerts and episodes of our podcast, *Triage*.

[6] "Health Care Providers" are defined for purposes of the Information Blocking Rule to include, inter alia, hospitals, skilled nursing facilities, nursing facilities, home health entities or other long term care facilities, health care clinics, community mental health centers, renal dialysis facilities, blood centers, ambulatory surgical centers, emergency medical services providers, federally qualified health centers, group practices, pharmacies, laboratories, physicians, and rural health clinics. See 45 C.F.R. § 171.102 (referencing 42 U.S. Code § 300jj).

[7] See 45 C.F.R. § 171.103. With regard to Information Blocking, the Cures Act treats certain actors differently in two significant ways: one is related to penalties, which differ if the actor is a Health Care Provider, as opposed to an HIE/HIN or Health IT Developer; and the second is related to the knowledge standard for whether a practice interferes with access, use, or exchange of EHI. Health Care Providers must actually know the practice is unreasonable and is likely to interfere with access, use, or exchange, whereas Health IT Developers and HIE/HINs are held to a "should know" standard. While we cannot speak for Congress, we believe this is a reflection of Congress's impression that Health IT Developers and HIEs/HINs behave more purposely in ways that block otherwise permissible access, exchange, or use of EHI by patients and providers. See also ONC, 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification, April 24, 2020, located here (visited August 30, 2020).

[8] See 45 C.F.R. § 171.102. The Final Rule combines previously proposed actions "to materially discourage" and "prevent" into one standard of "interfere with," and in fact ONC has indicated that it will implement technical corrections to section 171.103(a)(2), which inadvertently carried over the previous standard into the Final Rule. See 85 Fed. Reg. 25,642, 25,809 (May 1, 2020); see also ONC, 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification, April 24, 2020, located here (visited August 30, 2020).

[9] 85 Fed. Reg. at 25,811-8; 84 Fed. Reg. 7,424, 7,518-21 (Mar. 4, 2019).

©2005-2026 K&L Gates LLP. All Rights Reserved.

[10] 85 Fed. Reg. at 25,812.

[11] 45 C.F.R. § 171.102(a)(1).

[12] 85 Fed. Reg. at 25,814.

[13] Id.

[14] 45 C.F.R. § 171.201.

[15] 45 C.F.R. § 171.202.

[16] 45 C.F.R. § 171.203.

[17] 45 C.F.R. § 171.204.

[18] 45 C.F.R. § 171.205.

[19] 45 C.F.R. § 171.301.

[20] 45 C.F.R. § 171.302.

[21] 45 C.F.R. § 171.303.

[22] 84 Fed. Reg. 7424, 7518 (March 09, 2019).

[23] 85 Fed. Reg. at 25,649.

[24] While ONC has indicated that, due to the COVID-19 national pandemic, it will exercise discretion in enforcing key components of the ONC Health IT Certification Program, codified at 45 C.F.R. Part 170, until three months after each initial compliance date or timeline as outlined in the Final Rule, it has not extended compliance deadlines for the Information Blocking Rule at 45 C.F.R. Part 171.

[25] ONC replaced the Common Clinical Data Standards (CCDS) data elements with USCDI data elements, effective for access, use, and exchange of EHI for purposes of the Information Blocking Rule as of November 02, 2020. USCDI data elements are as follows: (1) allergies and intolerances, (2) assessment and plan of treatment, (3) care team member(s), (4) clinical notes, (5) goals, (6) health concerns, (7) immunizations, (8) laboratory, (9) medications, (10) patient demographics, (11) problems, (12) procedures, (13) provenance, (14) smoking status, (15) unique device identifier(s) (UDIs) for a patient's implantable device(s), and (16) vital signs. See ONC, United States Core Data for Interoperability (available here, accessed Aug. 28, 2020). Some data elements have been removed, others will be removed over time, and three data elements have been added: clinical notes, certain patient demographics, and provenance. For more information, see 85 Fed. Reg. at 25,644; ONC, 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification, April 24, 2020, located here (visited August 30, 2020).

[26] 45 C.F.R. § 171.103.

[27] See ONC, United States Core Data for Interoperability (available here, accessed Aug. 28, 2020).

[28] 45 C.F.R. § 171.102.

[29] 85 Fed. Reg. at 25793.

[30] The Content and Manner Exception indicates that an actor must respond to a request for access, use, or

©2005-2026 K&L Gates LLP. All Rights Reserved.

exchange of EHI in an manner requested with EHI identified by the data elements represented in the USCDI standard through May of 2022, and after that by all EHI in a Designated Record Set (as defined by HIPAA's Privacy Rule), unless the actor is technically unable to fulfill such request. 45 C.F.R. § 171.301. We will provide additional guidance on the Content and Manner Exception and its interplay with the new USCDI data elements in a coming Triage podcast.

[31] See 85 Fed. Reg. at 25,842.

[32] Id. See also 45 C.F.R. § 171.201.

[33] See 45 C.F.R. § 171.103(a)(1).

[34] See The 21st Century Cures Act, Pub. L. No. 114-255, Sec. 3002, 130 Stat. 1178 (2016) (codified at 42 U.S.C. 300jj-14); see also, ONC, 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Final Rule: Information Blocking, (available here, accessed Aug. 10, 2020).

[35] See 85 Fed. Reg. at 25,789.

[36] See 85 Fed. Reg. 22,979, 22,989-92 (April 24, 2020).

[37] See 85 Fed. Reg. at 25,652 (May 1, 2020).

[38] While ONC has indicated that, due to the COVID-19 national pandemic, it will exercise discretion in enforcing key components of the ONC Health IT Certification Program, codified at 45 C.F.R. Part 170, until three months after each initial compliance date or timeline as outlined in the Final Rule, it has not extended compliance deadlines for the Information Blocking Rule at 45 C.F.R. Part 171.

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.

©2005-2026 K&L Gates LLP. All Rights Reserved.