COSMOS
Navigate the Compliance Universe

Complete Healthcare Compliance Manual 2025
Health Information Management: Patient Access, Information Blocking, and the 21st Century Cures Act

By Patricia A. Markus,[1] JD, CIPP/US

What Are the Patient Access and Information Blocking Requirements of the 21st Century Cures Act?

Since 2003, under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, individuals have had the right to access and obtain a copy of their own protected health information (PHI) from a healthcare provider or a provider's business associate, subject to a few narrow exceptions.[2] However, due to a misunderstanding of HIPAA requirements and, in some cases, a desire to protect against competition, providers over the last few years have repeatedly been fined by federal regulators for Privacy Rule infractions. These include failing to provide access to PHI in a timely manner; denying access when access is permitted; failing to provide access in the format requested; failing to provide access to individuals' personal representatives as required by HIPAA; and charging excessive fees for copies of medical records.[3]

More recently, regulations under the 21st Century Cures Act (Cures Act), which prohibit healthcare providers from engaging in "information blocking," have complicated whether and how providers give access to individuals' electronic health information (EHI).[4] The final rule addresses interoperability, information blocking, and the Office of the National Coordinator for Health Information Technology (ONC) Health IT Certification Program under the Cures Act. The final rule was published in the *Federal Register* on May 1, 2020, and, following a six-month implementation delay due to COVID-19, became effective on April 5, 2021.[5] The information blocking provisions of the Cures Act responded to concerns about healthcare industry practices that were unreasonably limiting the availability and use of EHI for permitted purposes, including use by individuals and other appropriate persons within the healthcare ecosystem.[6] These industry practices include contract terms, policies, or processes that interfered with individuals' rights to access their own PHI for permitted purposes under HIPAA; fees that made the access, exchange, or use of PHI cost prohibitive; and nonstandard implementation of health information technology that substantially increased the cost, complexity, and burden of sharing health data.

A significant emphasis in the Cures Act's Information Blocking Rule is ensuring the rights of individuals and their personal representatives to access their PHI without unnecessary delay, without special effort on the individuals' part, and at a minimal cost or, in certain circumstances, no cost. This protection of individuals' right of access expands upon the right originally set forth in the HIPAA Privacy Rule and furthered by the Health Information Technology for Economic and Clinical Health Act (HITECH). The Information Blocking (IB) Rule builds upon this right of access; it prohibits charging individuals, their personal representatives, or another person or designated entity for providing "electronic access" to the individual's EHI.

Compliance with the IB Rule requires a paradigm shift in the way healthcare industry stakeholders and compliance officials think about when and how to make EHI available to third parties. For 19 years, the healthcare industry worked with the HIPAA Privacy Rule, which specifies when PHI may be used and disclosed. The IB Rule, on the other hand, requires healthcare providers and others governed by the rule to make EHI available for access, use, or

disclosure when appropriate to do so and when not otherwise prohibited by law. Thus, the analysis regarding whether to use and disclose PHI in certain situations transitions from the HIPAA-based presumption that PHI should not be used or disclosed unless doing so is specifically permitted or required, to a presumption that EHI must be made available unless the access, use, or disclosure is specifically *prohibited* by law or if the circumstances surrounding the decision not to make EHI available fit within an exception to the definition of information blocking.

The IB Rule includes a significant number of defined terms that need to be understood to determine what conduct may be problematic and what conduct may fall within one of its eight exceptions. Before the enforcement mechanisms for the IB Rule are finalized, compliance officers need to understand the requirements of the IB Rule and the limitations of its exceptions. Simultaneously, compliance officers must watch for guidance to be issued by the ONC and other agencies within the U.S. Department of Health and Human Services (HHS) that address how to comply with different aspects of the rule and its exceptions.

Risk Area Governance

The IB Rule generally prohibits "actors" from engaging in "information blocking." Its definition of "actor" includes a healthcare provider, a developer of certified health IT, and a health information network or a health information exchange (HIE). (Health information *networks* and health information *exchanges* are collectively referred to as HIEs).[7] The term "information blocking" is defined, in part, as a practice that, except as required by law or covered by an exception set forth in the IB Rule, "is likely to interfere with access, exchange, or use of electronic health information."[8] "Interfere with" means to prevent, materially discourage, or otherwise inhibit.[9] A "practice" is defined as "an act or omission by an actor."[10]

The IB Rule is an intent-based statute. This means that an actor engages in information blocking only if the actor (while engaging in a practice that is likely to interfere with access, exchange, or use of EHI) has the level of intent specified in the IB Rule. *Healthcare providers* engage in information blocking only if they know that the practice is unreasonable and is likely to interfere with the access, exchange, or use of EHI.[11] *Health IT developers and HIEs* engage in information blocking only if they know or should know that a practice is likely to interfere with the access, exchange, or use of EHI.[12]

EHI was not defined in the Cures Act or the other statutes to which it refers,[13] so a definition of EHI was included in the IB Rule.[14] The definition of EHI is a subset of electronic protected health information (ePHI) as defined in the HIPAA Privacy Rule,[15] in that EHI is limited to ePHI that would be included in a designated record set (DRS), whether or not the actor is a HIPAA-covered entity.[16] The Privacy Rule defines a designated record set as follows:

1. A group of records maintained by or for a **covered entity** that involve:
    i. Medical and billing records about individuals and maintained by or for a covered healthcare provider;
    ii. Enrollment, payment, claims adjudication, and case or medical management record systems that are maintained by or for a health plan or are used, in whole or in part, by or for the covered entity to make decisions about individuals.
2. The term "record" here means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a **covered entity**.[17]

The definition of EHI specifically *excludes* psychotherapy notes and information compiled in anticipation of or for

use in a civil, criminal, or administrative action or proceeding.[18]

The ONC did not limit the scope of EHI to records that are used or maintained by or for covered entities: "actors" who are regulated by the IB Rule include noncovered entities such as HIEs, certified health IT developers, and healthcare providers who do not take insurance. This, in turn, means that what constitutes EHI is much broader than the definition of ePHI under HIPAA: EHI may encompass medical and billing records, health plan records, and other records used to make decisions about individuals when such records are maintained by developers of certified health IT, HIEs, and healthcare providers that are not covered entities.

Related Laws

Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191 (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health Act of 2009, Pub. L. No. 111–5 (HITECH)

Although HIPAA restricts the unauthorized use and disclosure of patients' PHI, it expressly requires covered entities and business associates to provide individuals and their personal representatives access to such individuals' PHI in a DRS, with the exception of psychotherapy notes[19] and information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.[20] After an individual requests access, under the HITECH Act's implementing regulations, a covered entity or business associate must act on the request within 30 days, unless the entity is unable to make the information available within that period (e.g., if the information is stored offsite or must be compiled from a variety of paper and electronic files). In that instance, the entity has an additional 30 days to provide access to the PHI if it notifies the individual and states the reason for the delay and the expected date on which the PHI will be provided.[21] The HITECH regulations also specify that any fee to produce an electronic copy of PHI may not be greater than the labor costs involved in responding to the request for the copy plus any costs for supplies for creating an electronic copy on portable media.[22] HITECH additionally requires providers, upon an individual's request, to send a copy of PHI directly to a person or entity designated individual so long as the individual's request to do so is "clear, conspicuous, and specific."[23] Finally, HITECH requires covered entities and business associates to provide access to PHI in the *form and format* (e.g., electronically on a flash drive) requested by the individual, if feasible. If doing so is not feasible, the entity must provide the PHI in a readable form and format agreed upon by the entity and the requestor.[24]

Common Compliance Risks

Information Blocking Examples

The Final Rule specifies that an action or practice by an actor "implicates" information blocking if the practice limits—by contract, license, or policy—availability of EHI that is not prohibited from being made available, or if the practice involves either ignoring a request to share information or charging an exorbitant sum to make EHI available. ***Implicates*** does not necessarily mean ***violates***. As with HIPAA, where a violation is not necessarily a reportable breach, a practice that implicates the IB Rule may not violate the rule, but a fact-specific evaluation must be undertaken to determine whether such an action or practice is required by law or complies with an exception to the IB Rule.

A few examples of practices that "implicate" the IB Rule include:

- A hospital's internal policy requiring staff to obtain the patient's written consent before sharing the patient's EHI with unaffiliated providers for treatment, where such consent is not required by law.

- A practice's failure, upon receiving a patient's request, to forward the patient's EHI to a former shareholder of the practice who recently joined a competitor practice.
- A hospital's choosing not to enable a function of its patient portal that allows patients to transmit their EHI directly to third parties. A practice's ignoring or unreasonably delaying response to a request for EHI.

Exceptions to Information Blocking

The ONC has identified eight exceptions to the IB Rule describing "reasonable and necessary" practices that do not constitute information blocking. The exceptions apply to certain activities that are likely to interfere with, prevent, or materially discourage the access, exchange, or use of EHI, but that would be reasonable and necessary if certain conditions are met. The first five exceptions involve *not fulfilling requests* to access, exchange, or use EHI, while the final three exceptions specify procedures for *fulfilling requests* to access, exchange, or use EHI.[25] An actor's practice that does not meet the conditions of an exception will not automatically constitute information blocking; the practice will be evaluated on a case-by-case basis to determine whether the practice rises to the level of an interference and whether the actor acted with the requisite intent.[26]

a. Preventing Harm Exception

b. Objective: This exception recognizes that the public interest in protecting patients and other persons against unreasonable risks of harm can justify practices that are likely to interfere with access, exchange, or use of EHI.[27]

c. Exception and Key Conditions: Under this exception, a provider may refuse to make EHI available if it has a reasonable belief denying access will substantially reduce risk of harm to a patient or another person that otherwise would arise from making the EHI available. The risk must be that corrupt or inaccurate data will be included in a patient's record or that, based on a licensed professional's determination, disclosing EHI is likely to endanger the life or physical safety of the patient or others. A provider's practice involved in refusing to make EHI available must be no broader than necessary to substantially reduce the risk of harm that the practice is implemented to reduce, and the provider's practice must either be based on an organizational policy or on an individual determination that concerns the circumstances of an incident. Specific additional criteria apply.[28]

d. The Privacy Exception

e. Objective: This exception recognizes that if an actor is permitted to provide access, exchange, or use of EHI under a privacy law, then the actor should do so. However, an actor should not be required to use or disclose EHI in a manner that is prohibited under state or federal privacy laws.[29]

f. Exception and Key Conditions: Under this exception, a provider may refuse to make EHI available if (i) federal or state privacy laws impose preconditions to access (such as consents or authorizations) that have not been satisfied; (ii) HIPAA allows the provider to deny access to an individual; or (iii) the patient has requested that their information not be shared. In each circumstance, specific additional conditions apply.[30]

g. The Security Exception

h. Objective: This exception is intended to cover all legitimate security practices by actors; however, it does not prescribe a maximum level of security or dictate a one-size-fits-all approach.[31]

i. Exception and Key Conditions: Under this exception, a provider may refuse to make EHI available if doing so

is necessary to safeguard the confidentiality, integrity, and availability of the EHI consistent either with (i) the provider's organizational policies or (ii) a specific determination that no reasonable, less-obstructive alternatives exist for securing the EHI. The practice must directly relate to safeguarding the confidentiality, integrity, and availability of EHI and be tailored to specific security risks.[32]

j. Infeasibility Exception

k. Objective: This exception recognizes that legitimate and practical challenges may limit an actor's ability to comply with requests for access, exchange, or use of EHI.[33]

l. Exception and Key Conditions: Under this exception, a provider may refuse to make EHI available if (i) an extraordinary event beyond its control (i.e., a natural disaster) prevents it from fulfilling the request for access; (ii) it cannot segregate the requested EHI from other information that is not subject to access (e.g., the other information that may not be disclosed pursuant to law); or (iii) it shows that responding to the request is not feasible (e.g., due to the type of information sought, the cost involved in providing it, available resources, and many other factors).[34]

m. Note: To meet this exception, within 10 days of receiving a request for access, a provider must notify the requestor in writing of the reason why it is infeasible to provide the access sought.

n. Health IT Performance Exception

o. Objective: This exception recognizes that for health IT to perform properly and efficiently, it must be maintained, and in some instances improved. This may require that health IT be taken offline temporarily. Actors should not be deterred from taking reasonable and necessary measures to make health IT temporarily unavailable or to degrade the health IT's performance for the benefit of the overall performance of health IT.[35]

p. Exception and Key Conditions: Under this exception, a provider is not engaging in information blocking if it takes reasonable and necessary measures to make health IT temporarily unavailable, so long as such unavailability lasts no longer than necessary and is in accordance with additional conditions.[36]

q. Note: If a provider is acting as a health IT developer or an HIE, it may temporarily block access to EHI if necessary for maintenance of the platform/system and to improve health IT performance. The unavailability may be for no longer than necessary.[37]

r. The Content and Manner Exception

s. Objective: This exception provides clarity and flexibility regarding the required*content* (i.e., scope of EHI) of an actor's response to a request to access, exchange, or use EHI and the *manner* in which the actor may fulfill the request.[38]

t. Exception and Key Conditions: Under this exception, a provider generally must provide access to EHI in the manner requested, unless the provider is technically unable to fulfill the request or cannot reach agreeable terms with the requestor. If unable to provide access as requested or as agreed, the provider must take reasonable steps to fulfill the request in an alternative manner, consistent with additional specified technical standards. The requirements of the "Fees and Licensing" exceptions will apply to such alternative access.[39]

u. Fees Exception

v. Objective: This exception enables actors to charge fees related to the development of technologies and the provision of services that enhance interoperability, while not protecting rent-seeking, opportunistic fees, or exclusionary practices that interfere with access, exchange, or use of EHI.[40]

w. Exception and Key Conditions: Under this exception, a provider may charge a reasonable fee for making EHI available, as long as the fee is based on its costs and applied to similarly situated requestors in a nondiscriminatory manner. Other standards apply.[41]

x. Note: Providers may not charge a fee "based in any part on the electronic access of an individual's EHI" by individuals, their personal representatives, or another person or entity designated by such individuals.[42] "Electronic access" means an "internet-based method" that makes EHI available at the time EHI is requested "and where no manual effort is required to fulfill the request."[43] An example of electronic access is a healthcare provider's patient portal.

y. Licensing Exception

z. Objective: This exception allows actors to protect the value of their innovations and charge reasonable royalties in order to earn returns on the investments they have made to develop, maintain, and update those innovations.[44]

aa. Exception and Key Conditions: Under this exception, a provider must agree to license certain technologies (***"interoperability elements"***), which include certified EHR technology and most application programming interfaces (APIs), as well as hardware, software, intellectual property, upgrades, or services controlled by the provider that may be necessary to access, exchange, or use EHI that enable access to EHI upon a third party's request for a license, except where the third party intends to develop a competing product through the license. Any license fees must be reasonable, and the license terms must be nondiscriminatory. Certain other limitations apply.[45]

ab. Note: To meet this exception, within 10 business days of receipt of a request for a license of interoperability elements, a provider must begin negotiations for such a license and work in good faith to conclude such negotiations within 30 business days.

Addressing Compliance Risks

Areas to Prioritize

The IB Rule states that information blocking will "almost always" be implicated if an actor's practice interferes with access, exchange, or use of EHI for any of these purposes that follow.[46] It may be efficient, therefore, for compliance officers to prioritize compliance activities with respect to the following areas:

1. Ensure that policies and practices generally do not inappropriately delay or unreasonably restrict sharing of EHI. In this regard, be sure that:
    a. Patients may access their own EHI and exchange and use it without special effort.
    b. Healthcare professionals and other authorized persons have the EHI they need, when and where they need it, to make treatment decisions, coordinate/manage care, and use the EHI they receive from other sources.
    c. Payers and other purchasers of healthcare services can obtain EHI needed to effectively assess clinical

value and promote transparency regarding quality and costs.

d. Healthcare providers can access, exchange, and use EHI for quality improvement and population health management.

e. EHI is made available for patient safety and public health.

2. Evaluate for possible information blocking the provider's policies and practices involving the availability of EHI. Determine whether an exception applies in each instance.

3. Compare operational policy provisions (including HIPAA policies) to IB Rule requirements; update policies where needed. Examples include the following:

f. Preventing Harm Exception

i. Review policy on individual's right to access information. Ensure that it includes provisions that conform to the exception regarding preventing harm. Examples could include situations involving abuse (when access is requested by a parent or personal representative) or when a clinician has determined a risk of harm to the individual or another person.

ii. Remember that the exception will be met with either a policy outlining limitations that are no broader than needed to prevent harm or with an individualized determination of harm in a given circumstance.

iii. Evaluate how quickly test results are made available to individuals and consider creating a policy noting that test results will be made available without delay unless a clinician makes a good faith, individualized determination of a substantial likelihood of harm arising in a given instance.

1. Individualized determinations should be *documentedin writing* (to defend against potential information-blocking complaints) and *maintained* in the patient's record. Some providers are working with their electronic health record system vendors to add drop-down menus that enable clinicians to describe individualized determinations of harm in different circumstances.

2. Be cautious about implementing a policy stating that certain categories of test results will be delayed—unless such delays are required by other laws (i.e., state law).

g. Privacy Exception

iv. Revise (or create) policies for notifying patients or others requesting EHI that is subject to a precondition when the consent or authorization that was submitted to satisfy the precondition requires modifications. Consider providing requestors a form that satisfies the elements of the required consent/authorization or other precondition when appropriate to do so.

v. Determine whether and how information about minors may be appropriate to make available but needs to be withheld when required by law (use the Infeasibility or Content and Manner Exceptions as needed).

h. Security Exception

vi. Consider whether terms in Business Associate Agreements (BAAs) and other documents that

address information security improperly interfere with the access, exchange, or use of EHI (i.e., are unreasonable or improperly obstructive). Update where necessary.

i. Infeasibility Exception

vii. Identify situations where data segmentation may be needed to comply with requests for access to EHI while also staying compliant with applicable laws that restrict such access, but where such segmentation isn't feasible. This might include documents scanned into a provider's system that contain some information that, by law, may not be disclosed.

viii. When a request is determined to be infeasible, ensure that the provider has a process for responding in writing within 10 business days of receiving the request.

ix. Remember that EHI may be made available in an alternative fashion if possible (and if the recipient agrees) under the Content and Manner Exception; in such a case, the provider will be subject to the requirements of the Fees and Licensing Exceptions if EHI is made available in an alternative fashion.

j. Health IT Performance Exception

x. Determine whether service-level agreements and other uptime standards in technology contracts—both in instances where the provider is the recipient of the software/services and where it is responsible for providing them (if any)—comply with the requirements of the exception.

k. Fees Exception

xi. Establish processes to evaluate and respond to requests for access to EHI, and determine appropriate costs for or limitations of such access.

xii. Where no manual effort is needed to provide electronic access to EHI, **individuals and their personal or legal representatives may not be charged a fee**. Review policies and processes regarding fees for making EHI available; update them as needed, ensuring that fees are reasonable. (Note that manual effort includes collating or assembling EHI from various systems in response to a request.)

xiii. In licensing contracts, the parties should agree in advance (i.e., at the time the contract is signed) on the fee, if any, for export or conversion of the requestor's data.

l. Licensing Exception

xiv. Determine what hardware, software, or services a provider may license to third parties that are "interoperability elements."

xv. Identify and revise contract terms and conditions that discourage the use of interoperability elements.

xvi. If applicable, establish policies for responding to requests from third parties for licenses of interoperability elements. Remember that actors have 10 business days to start license negotiations after a request and they have 30 business days to complete those negotiations in good faith.

xvii. Review the functionality of platforms and systems containing EHI. Ensure that such functionality has not been configured or disabled in a manner that would constitute information blocking. For example, check whether some physicians or physician offices provide patients their clinical notes while others do not or have not configured their systems to permit sharing of such information.

m. Licensing and Fee Exceptions

xviii. Assess whether pricing and fees in contracts that address access to EHI or licensing interoperability elements are appropriate or need modification.

xix. Remember that pricing may not be discriminatory and that the licensor may not, as a condition of offering the license, require the licensee to obtain other licenses or products that are unrelated to the requested interoperability elements or to give away the licensee's intellectual property.

4. Identify capabilities and limitations of platforms and systems containing EHI that could justify a denial of certain requests for access. For example, if the version of software used doesn't permit the export of EHI in a certain file format or can't otherwise accommodate a request for EHI and it is cost-prohibitive to upgrade to a different version of the software (and where the upgrade isn't required to comply with other laws).

5. Respond appropriately to requests for sharing of EHI. Develop a process for routing different requests to an individual or group of individuals who understand the requirements of the IB rule and who can set in motion an appropriate response to such requests

6. Plan to identify and educate personnel within multiple departments who are likely to be affected, including clinicians and individuals in the C-suite, as well as staff in finance, legal, IT, contracts, risk management, and records management. Those involved in contracting, compliance, IT, patient care, and health information management likely will require more robust education, but other leaders certainly should be aware of the new rule and its implications and should participate in decisions regarding compliance, where appropriate. All employees should be trained on which personnel (e.g., supervisor, department head) to contact about possible information-blocking concerns.

Possible Penalties

Penalties or other consequences for information blocking will apply depending on the type of actor involved in the activity that is determined to constitute information blocking. HIEs and developers of certified health IT are subject to substantial monetary penalties of up to a million dollars per violation, with the Office of Inspector General (OIG) serving as the enforcement agency. The OIG has yet to issue a final rule to establish parameters and enforcement dates pertaining to the civil monetary penalties to which health IT developers and HIEs will be subjected. The penalty determination will take into account factors such as the nature and extent of the information blocking and the resultant harm, including the number of patients and providers affected and the number of days the information blocking persisted.[47] Healthcare providers will be subject to different penalties and "appropriate disincentives" for information blocking, but these penalties and disincentives have not yet been definitively identified.

Significantly, an entity might fall into more than one category of actor depending on its activities. For example, a healthcare provider may also operate an HIE or fall within the definition of a developer of certified health IT; if the provider violates the IB Rule when it is acting as an HIE or developer of certified health IT, it will be subject to the substantial civil monetary penalty described above.

Compliance Resources

Information about the 21st Century Cures Act's Information Blocking final rule for patients, providers, and IT developers, along with links to other resources can be found here:

https://www.healthit.gov/curesrule/.

Fact Sheets are located at https://www.healthit.gov/curesrule/resources/fact-sheets are particularly useful.

Look for additional guidance from ONC and CMS on the rules at these web sites:
https://www.healthit.gov/topic/information-blocking and
https://www.healthit.gov/curesrule/resources/information-blocking-faqs.

Such guidance has been promised and will be needed to understand the nuances of the IB Rule and its interplay with HIPAA.

Risk Takeaways

- **Main points of interest:**
    - Individuals have had the right under HIPAA since 2003 to access and obtain copies of their health information, with limited exceptions.
    - The IB Rule enhances individuals' rights of access to their health information but makes determining when to share information with individuals, and others permitted to receive it, more challenging.
    - The exceptions to the IB Rule provide "safe harbors" against allegations of information blocking if complied with in their entirety.
- **Areas to watch:**
    - Avoid improperly withholding or delaying the provision of copies of EHI from individuals and their personal representatives, as OCR is receiving and investigating a wide variety of complaints in this area.
    - Be on the lookout for updated FAQs from ONC addressing the IB Rule.
    - Be on the lookout for more information from OIG and CMS regarding penalties that may be imposed under the IB Rule and the date on which such penalties may start.
- **Laws that apply:**
    - 21st Century Cures Act
    - HIPAA, as amended by the HITECH Act
- **Addressing compliance risks**:

- Review HIPAA policies for compliance with the IB Rule and its exceptions, and update or create new policies as needed.
- Review IT systems to determine how information may be shared from them, and review contracts to ensure that they do not implicate the IB Rule.
- Educate all members of the organization regarding who to contact if there is a question about releasing PHI.

1 Patricia A. Markus is a partner in the Raleigh office of Nelson Mullins Riley & Scarborough LLP. She represents healthcare providers and health technology companies on wide-ranging regulatory compliance, reimbursement, licensure, and operational matters. She regularly advises clients on ways to use technology to improve healthcare access and outcomes while assuring compliance with applicable data privacy and security laws and other healthcare regulatory requirements. Trish serves as the President-Elect of the American Health Law Association for 2022–2023.
2 45 C.F.R. § 164.524.
3 U.S. Department of Health & Human Services, Office of Civil Rights, "OCR Settles Three Cases with Dental Practices for Patient Right of Access under HIPAA," September 20, 2022, https://www.hhs.gov/about/news/2022/09/20/ocr-settles-three-cases-dental-practices-patient-right-access-under-hipaa.html.U.S. Department of Health & Human Services, Office of Civil Rights, "Eleven Enforcement Actions Uphold Patients' Rights Under HIPAA," July 15, 2022, https://www.hhs.gov/about/news/2022/07/15/eleven-enforcement-actions-uphold-patients-rights-under-hipaa.html.
4 21st Century Cures Act, Pub. L. No. 114–255, § 4004, 130 Stat. 1033 (2016).
5 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, 85 Fed. Reg. 25642 (May 1, 2020) (codified at 45 C.F.R. §§ 170, 171), https://www.federalregister.gov/documents/2020/05/01/2020-07419/21st-century-cures-act-interoperability-information-blocking-and-the-onc-health-it-certification.
6 21st Century Cures Act, 85 Fed. Reg. at 25790.
7 45 C.F.R. § 171.102.
8 45 C.F.R. § 171.103.
9 45 C.F.R. § 171.102.
10 45 C.F.R. § 171.102.
11 45 C.F.R. § 171.103.
12 45 C.F.R. § 171.103.
13 21st Century Cures Act, 85 Fed. Reg. at 25803.
14 45 C.F.R. § 171.102.
15 45 C.F.R. § 160.103.
16 45 C.F.R. § 171.102.
17 45 C.F.R. § 164.501 (*emphasis added*).
18 45 C.F.R. § 171.102.
19 45 C.F.R. § 164.501. Psychotherapy notes are defined as notes recorded by a mental health professional documenting or analyzing a conversation during a counseling session, and which are separated from the remainder of the individual's medical record.
20 45 C.F.R. § 164.524(a)(1).
21 45 C.F.R. § 164.524(b)(2).
22 45 C.F.R. § 164.524(c)(4).
23 42 U.S.C. § 17935(e).

24 45 C.F.R. § 164.524(c)(2).

25 21st Century Cures Act, 85 Fed. Reg. at 25821.

26 21st Century Cures Act, 85 Fed. Reg. at 25820.

27 "Cures Act Final Rule Information Blocking Exceptions," Office of the National Coordinator for Health Information Technology, (last reviewed October 31, 2022), https://www.healthit.gov/sites/default/files/2022-07/InformationBlockingExceptions.pdf.

28 45 C.F.R. § 171.201.

29 45 C.F.R. § 171.202.

30 45 C.F.R. § 171.202.

31 45 C.F.R. § 171.203.

32 45 C.F.R. § 171.203.

33 45 C.F.R. § 171.204.

34 45 C.F.R. § 171.204.

35 45 C.F.R. § 171.205.

36 45 C.F.R. § 171.205.

37 45 C.F.R. § 171.205.

38 45 C.F.R. § 171.301.

39 45 C.F.R. § 171.301.

40 45 C.F.R. § 171.302.

41 45 C.F.R. § 171.301.

42 45 C.F.R. § 171.302(b)(2).

43 45 C.F.R. § 171.302(d).

44 45 C.F.R. § 171.303.

45 45 C.F.R. § 171.303.

46 21st Century Cures Act, 85 Fed. Reg. at 25810.

47 42 U.S.C. § 300jj–52(b)(2)(A).