healthcurrent

# Information Blocking Compliance Check-Up: Updating HIPAA Policies and Procedures

With the compliance deadline looming, it is important that health care providers subject their existing health information policies and practices to a check-up. This check-up will help providers identify their health information practices that might implicate the prohibition against information blocking. This educational document provides a framework to facilitate this check-up, including:

- An overview of the Information Blocking Rule (collectively, 42 U.S.C. § 300jj-52 and 45 C.F.R. Part 171);
- A summary of the conditions that must be met to qualify for the Preventing Harm, Privacy and Security Safe Harbors (defined below);
- A checklist of the most common HIPAA[1] Policies and Procedures that health care providers should review and consider updating to satisfy the documentation conditions of these Safe Harbors; and
- A few practice tips for updating HIPAA Policies and Procedure for alignment with the Safe Harbors.

## OVERVIEW OF THE INFORMATION BLOCKING RULE

The Information Blocking Rule prohibits certain actors, including health care providers, from engaging in practices that are likely to interfere with the access, exchange or use of electronic health information (EHI), unless the practice is required by law or a regulatory exception applies. We refer to the regulatory exceptions as "Safe Harbors."

The following are examples of practices that might implicate the prohibition against information blocking:

- Requiring a patient to sign a release of information before sharing the patient's EHI with unaffiliated providers for treatment purposes when the patient's consent is not required by state or federal law;
- Incorrectly claiming that HIPAA or other state and federal laws preclude a health care provider from exchanging EHI with unaffiliated providers;
- Delaying a patient's access to their EHI for several days, even though the provider has the ability to provide same day access to the EHI (such as through a patient portal); and
- Using written agreements (such as a HIPAA Business Associate Agreement, HIPAA Data Use Agreement, or other data sharing agreement) or policies and procedures to forbid, limit or delay disclosures that would otherwise be permissible under state and federal law.

This list is by no means exhaustive. Other practices—acts or omissions—that a health care provider knows are unreasonable and likely to interfere with the access, exchange or use of EHI will implicate the Information Blocking Rule and may be unlawful, unless the practice is required by law or is covered by a Safe Harbor.
If a practice qualifies for a Safe Harbor, an actor will have certainty that the practice will not violate the Information Blocking Rule. The Office of the National Coordinator for Health Information Technology (ONC) has created eight Safe Harbors that can be broken down into two categories:

| Not fulfilling EHI requests | Procedures for fulfilling EHI requests |
|---|---|
| Preventing Harm<br>Privacy<br>Security<br>Infeasibility | Content and Manner<br>Fees<br>Licensing |

To qualify for a Safe Harbor, an actor must meet all applicable conditions of the Safe Harbor at all relevant times. Three of the Safe Harbors—Preventing Harm, Privacy and Security—have documentation conditions that can be satisfied by following an organizational policy that meets the conditions of the applicable Safe Harbor. Actors bear the burden of showing that their EHI practices qualify for Safe Harbor protection.

ONC expects that health care providers that are HIPAA covered entities will be able to leverage their existing HIPAA Policies and Procedures to satisfy these documentation conditions. However, these HIPAA Policies and Procedures should be reviewed and updated for compliance with the conditions of these Safe Harbors and the other potentially applicable Safe Harbors.

Failing to meet the conditions of a Safe Harbor does not mean that a practice violates the Information Blocking Rule. The Office of Inspector General (OIG) will evaluate practices on a case-by-case basis to determine if all the elements of an information blocking violation are present. If OIG determines that a health care provider has engaged in information blocking, OIG will refer that provider to the appropriate agency for disincentives. It is therefore in a provider's best interests to align its EHI practices—including organizational policies and procedures—with the Safe Harbors to avoid the risk and uncertainty associated with OIG case-by-case investigations.

## THE PREVENTING HARM, PRIVACY AND SECURITY SAFE HARBORS

### Preventing Harm Safe Harbor[2]

It will not be information blocking if an actor engages in practices that are reasonable and necessary to prevent harm to a patient or another person, so long as the regulatory conditions are met. To qualify for the Preventing Harm Safe Harbor, an actor must demonstrate all of the following conditions have been met:

- ✓ A reasonable belief that the actor's practice substantially reduces a risk of harm to the patient who is the subject of the EHI or another natural person.

- ✓ The practice is no broader than what is necessary to substantially reduce the risk of harm.

- ✓ The risk of harm must be reasonably likely and fall into one of the following two categories:
  - The risk of harm is determined on an individualized basis by a licensed health care professional who has a past or current clinician-patient relationship with the patient whose EHI is at issue, and who is exercising his or her professional judgment. In this case, the denial must be implemented consistently with a patient's right to have the denial reviewed in a manner consistent with HIPAA's review provisions or other law that might apply to the actor.
  - The risk of harm is from data that is known or reasonably suspected to be wrong, such as mismatched data arising from misidentification of the patient or patient's EHI, corrupt data because of technical failures, or inaccurate data recorded/incorporated in EHI.

- ✓ The type of harm must be the same type of harm under which a licensed health care professional may issue a reviewable denial of an individual's access request under HIPAA. The harm standard required—*i.e.*, "substantial harm" or "harm to the life or physical safety"—depends on the practice at issue. For instance:
  - If the practice interferes with the access, exchange or use of EHI by a **patient's legal representative** (such as a personal representative), and the **denial involves an individualized determination of harm**, then the harm standard is **substantial harm to the patient or another person**;
  - If the practice interferes with the access, exchange or use of EHI by a **patient or the patient's legal representative**, and the **denial involves an individual determination of harm involving EHI**

**referencing another natural person**, then the harm standard is **substantial harm to that other person**;
- If the practice interferes with the access, exchange or use of EHI by a **patient**, then the harm standard is **harm to the life or physical safety of the patient or other natural person**; or
- If the practice interferes with **any other legally permissible** access, exchange or use of EHI not covered above, then the harm standard is **harm to the life or physical safety of the patient or other natural person**.

✓ The practice must be based on one of the following, either a:
- Written organizational policy. The written policy must be:
  - Based on relevant clinical, technical, and other appropriate expertise; and
  - Implemented in a consistent and non-discriminatory manner; and
  - Conform to the conditions listed above.
- Fact specific determination. Fact specific determinations must be:
  - Based on facts and circumstances known or reasonably believed by the actor at the time the determination was made and while the practice remains in use; and
  - On expertise relevant to implementing the practice consistent with the conditions listed above.

## Privacy Safe Harbor: Legal Preconditions[3]

There are four components (or sub-exceptions) contained within the Privacy Safe Harbor. One of those sub-exceptions applies in situations where state or federal law requires that a certain legal precondition (or multiple preconditions) be met before an actor can provide access, exchange or use of EHI. Under these circumstances, it will not be information blocking if an actor's practice is reasonable and necessary to satisfy a legal precondition, so long as the conditions of this Safe Harbor are met. Examples of common legal preconditions include patient consent or authorization for the disclosure or verification of the EHI requestor's identity or authority.

To qualify for this Safe Harbor, an actor must demonstrate that the practice meets all of the following conditions:

✓ It is implemented in a consistent and non-discriminatory manner;

✓ It is tailored to the applicable precondition; and

✓ It is based on one of the following, either a:

- Written organizational policy. The written policy must:
  - Specify the criteria to be used by the actor to determine when the precondition would be satisfied and the steps that the actor will take to satisfy the precondition; and
  - The policy must be implemented, including through workforce member training on the policy.
- A fact specific determination. Fact specific determinations must be:
  - Based on facts and circumstances known or reasonably believed by the actor at the time the determination was made identifying the criteria used by the actor to determine when the precondition would be satisfied;
  - Any criteria that were not met; and
  - The reason why the criteria were not met.

If an actor is subject to multiple laws that have inconsistent legal preconditions, an actor can meet these documentation requirements by adopting and implementing a uniform set of privacy policies and procedures that follow the most restrictive preconditions. For instance, if a mental health care provider

operates in States A, B and C, and State A requires patient consent for treatment disclosures of mental health information to a patient's other providers, but States B and C do not, the provider could adopt a privacy policy that requires patient consent for treatment disclosures that uniformly applies in States A, B and C.

In circumstances where the legal precondition to be satisfied is obtaining the patient's consent or authorization, and the actor has received a **consent or authorization that does not satisfy the legal elements necessary for a valid consent or authorization**, the actor must:

- ✓ Use reasonable efforts within its control to provide the individual with a consent or authorization form that satisfies all required elements of the precondition or provide other reasonable assistance to the individual to satisfy all required elements of the precondition; and

- ✓ Not improperly encourage or induce the individual to withhold the consent or authorization.

If the legal precondition relates to **verification** of an EHI requestor's identity or authority, a health care provider must be careful to tailor its verification procedures to satisfy the legal requirement without unreasonably interfering with the requestor's access, exchange or use of EHI. For example, a policy that a driver's license is the only acceptable form of identification (as opposed to other types of legally acceptable forms of identification such as a valid passport), is not appropriately tailored because the provider's preference for one form of government-issued identification over another does not meaningfully address the legal precondition.

## Security Safe Harbor[4]

It will not be information blocking if a practice is reasonable and necessary to protect the security of EHI, so long as the regulatory conditions of the Security Safe Harbor are met. Examples of practices that might qualify for this Safe Harbor include practices that are in direct response to a known security threat or used to verify a person's identity. To qualify for the Security Safe Harbor, an actor must demonstrate that the practice satisfies all of the following conditions:

- ✓ It is directly related to safeguarding confidentiality, integrity and availability of EHI;

- ✓ It is tailored to the specific security risk being addressed;

- ✓ It is implemented in a consistent and non-discriminatory manner; and

- ✓ It is based on one of the following, either a:

    - Written organizational policy. The written policy must be:
        - Prepared on the basis of, and be directly responsive to, security risks identified and assessed by or on behalf of the actor;
        - Align with one or more applicable consensus-based standards or best practice guidance (such as NIST-800-53 Rev. 5, the NIST Cybersecurity Framework, and NIST SP 800-100, SP 800-37 Rev. 2, SP 800-39, as updated and as interpreted through formal guidance);
        - Provide objective timeframes and other parameters for identifying, responding to, and addressing security incidents; and
        - Conform to the conditions listed above.

    - Fact specific determination. Fact specific determinations must be:

- Based on facts and circumstances known or reasonably believed by the actor at the time the determination was made, that the practice is necessary to mitigate the security risk to EHI; and
- There are no reasonable and appropriate alternatives to the practice that address the security risk that are less likely to interfere with the access, exchange or use of EHI.

Additionally, ONC provides that it will not be information blocking for actors to provide notifications or patient education regarding the privacy and security practices of third party applications selected by a patient to obtain access to the patient's EHI so long as the notification/education meets the following requirements:

- ✓ It focuses on the current privacy and security risk posed by the technology or the third-party developer of the technology;

- ✓ It is factually accurate, unbiased, objective, and not unfair or deceptive; and

- ✓ It is provided in a non-discriminatory manner.

## HIPAA POLICIES AND PROCEDURES CHECKLIST

We specifically suggest reviewing and revising the following common HIPAA Policies and Procedures:

- ✓ HIPAA Definitions Policy

- ✓ HIPAA Use and Disclosure Policies and related procedures/forms, including but not limited to those relating to:
  - Use and disclosure of health information without individual authorization
  - Use and disclosure of health information for treatment, payment and health care operations
  - Required use and disclosure of health information
  - Use and disclosure of health information requiring individual authorization
  - Use and disclosure of sensitive health information
  - Minimum necessary standard procedures
  - Safeguards for use and disclosure/verification of identity and authority

- ✓ HIPAA Access Policies and related procedures, including but not limited to those relating to:
  - Individual access rights
  - Personal representatives

- ✓ HIPAA Security Policies and related procedures

- ✓ HIPAA Administrative Policies and related procedures, including but not limited to those relating to:
  - Designating a responsible individual for compliance (*e.g.*, Privacy Official)
  - Workforce training
  - Record retention
  - Reporting violations, internal investigations and mitigation
  - Prohibiton on retaliation
  - Sanctions for noncompliance
  - Cooperation in governmental investigations
  - Businesss associates and business associate agreements (BAA)
  - Data use agreements (DUA)

# PRACTICE TIPS FOR UPDATING HIPAA POLICIES AND PROCEDURES

## HIPAA Definitions Policy

Organizational HIPAA Policies and Procedures often refer back to an overarching definitions policy. However, many of the defined terms in the Information Blocking Rule are different from the HIPAA definitions of those same terms or concepts. Thus, it is important to indicate in either your Definitions Policy or within the specific policy or procedural documents, where certain terms mean something different with respect to compliance with the Information Blocking Rule. Here is a breakdown of some of the important definitional differences that we have identified:

| HIPAA Definitions and Standards | Information Blocking Rule Definitions |
|---|---|
| Access means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (This definition applies to "access" as used in this subpart, not as used in subparts D or E of this part.). 45 C.F.R. § 164.304.<br>Note: This definition of access only applies to the HIPAA Security Rule.[5]<br><br>(a) Standard: Access to protected health information—(1) Right of access. Except as otherwise provided in paragraph (a)(2) or (a)(3) of this section, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, except for . . . . 45 C.F.R. § 164.524.<br>Note: This is not a definition of access, but it is the concept of individual access expressed in the HIPAA Privacy Rule.[6] | Access means the ability or means necessary to make electronic health information available for exchange or use. 45 C.F.R. § 171.102. |
| Disclosure means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information. 45 C.F.R. § 160.103. | Note: The Information Blocking Rule does not use the term "disclose" or "disclosure," but its use of the terms "access" and "exchange" overlap with HIPAA's definition of "disclose."<br><br>Access means the ability or means necessary to make electronic health information available for exchange or use. 45 C.F.R. § 171.102.<br><br>Exchange means the ability for electronic health information to be transmitted between and among different technologies, systems, platforms, or networks. 45 C.F.R. § 171.102. |
| Electronic Protected Health Information means information that comes within paragraphs (1)(i) or (1)(ii) of the definition of protected health information. 45 C.F.R. § 160.103. | Electronic Health Information (EHI) means electronic protected health information as defined in 45 CFR § 160.103 to the extent that it would be included in a designated record set as defined in 45 CFR § 164.501, regardless of whether the group of records are used or |

| HIPAA Definitions and Standards | Information Blocking Rule Definitions |
|---|---|
| Protected health information means individually identifiable health information:<br>(1) Except as provided in paragraph (2) of this definition, that is:<br>(i) Transmitted by electronic media;<br>(ii) Maintained in electronic media; or<br>(iii) Transmitted or maintained in any other form or medium.<br>(2) Protected health information excludes individually identifiable health information:<br>(i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. § 1232g;<br>(ii) In records described at 20 U.S.C. § 1232g(a)(4)(B)(iv);<br>(iii) In employment records held by a covered entity in its role as employer; and<br>(iv) Regarding a person who has been deceased for more than 50 years. 45 C.F.R. § 160.103.<br><br>Designated Record Set means:<br>(1) A group of records maintained by or for a covered entity that is:<br>(i) The medical records and billing records about individuals maintained by or for a covered health care provider;<br>(ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or<br>(iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals.<br>(2) For purposes of this paragraph, the term record 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. 45 C.F.R. § 164.501.<br><br>Psychotherapy notes means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date. 45 C.F.R. § 164.501. | maintained by or for a covered entity as defined in 45 CFR § 160.103, but EHI shall not include:<br>(1) Psychotherapy notes as defined in 45 CFR § 164.501; or<br>(2) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding. 45 C.F.R. § 171.102.<br>Note: The scope of the Information Blocking Rule is limited to **electronic** PHI, which means it is much more limited in application than HIPAA. The Information Blocking Rule does not apply to a health care provider's paper records. |
| Health Care Provider means a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. § 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. § 1395x(s)), and any | Health Care Provider means a hospital, skilled nursing facility, nursing facility, home health entity or other long term care facility, health care clinic, community mental health center (as defined in section 300x–2(b)(1) of this |

| HIPAA Definitions and Standards | Information Blocking Rule Definitions |
|---|---|
| other person or organization who furnishes, bills, or is paid for health care in the normal course of business. 45 C.F.R. § 160.103 | title), renal dialysis facility, blood center, ambulatory surgical center described in section 1395l(i) of this title, emergency medical services provider, Federally qualified health center, group practice, a pharmacist, a pharmacy, a laboratory, a physician (as defined in section 1395x(r) of this title), a practitioner (as described in section 1395u(b)(18)(C) of this title), a provider operated by, or under contract with, the Indian Health Service or by an Indian tribe (as defined in the Indian Self-Determination and Education Assistance Act [25 U.S.C. § 5301 et seq.]), tribal organization, or urban Indian organization (as defined in section 1603 of title 25), a rural health clinic, a covered entity under section 256b of this title, an ambulatory surgical center described in section 1395l(i) of this title, a therapist (as defined in section 1395w–4(k)(3)(B)(iii) of this title), and any other category of health care facility, entity, practitioner, or clinician determined appropriate by the Secretary (through reference to 42 U.S.C. § 300jj). 45 C.F.R. § 171.102. |
| Covered Entity means:<br>(1) A health plan.<br>(2) A health care clearinghouse.<br>(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter. 45 C.F.R. § 160.103. | Actor means a health care provider, health IT developer of certified health IT, health information network or health information exchange. 45 C.F.R. § 171.102.<br>Note: Whether records are used or maintained by or for a HIPAA covered entity is not a determining factor for whether documents are EHI and subject to the Information Blocking Rule (see definition of EHI above). |
| Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information. 45 C.F.R. § 160.103. | Use means the ability for electronic health information, once accessed or exchanged, to be understood and acted upon. 45 C.F.R. § 171.102. |

## HIPAA Use and Disclosure Policies

HIPAA's rules surrounding the use and disclosure of EHI are permissive—a health care provider may (but is not required to) disclose EHI. By contrast, the Information Blocking Rule effectively requires health care providers to disclose EHI when it is requested, unless they are required by law not to or the practice of not disclosing or otherwise interfering with the disclosure falls within a Safe Harbor. We thus suggest updating HIPAA Use and Disclosure Policies to alert workforce members of this new obligation to disclose EHI if the disclosure is permitted under HIPAA and any other applicable state and federal laws.

We further suggest making the following updates to align these policies with the Safe Harbors:

- ✓ Consider removing requirements that workforce members first obtain a court order or a patient's signed authorization or consent before disclosing EHI, **if such requirements are not legally required by the laws that apply to you or your organization**. For example, HIPAA permits health care providers to

disclose EHI to a patient's other health care providers for treatment purposes without first obtaining the patient's signed authorization or consent. Thus, unless it is required by another state or federal law, requiring that a patient sign an authorization or consent to release the patient's EHI under these circumstances might implicate the Information Blocking Rule and this practice might not qualify for a Safe Harbor.

- ✓ Ensure that these HIPAA Use and Disclosure Policies include procedural checklists for confirming that legal preconditions have been met. For example, update these HIPAA Use and Disclosure Policies to:
  - Specify criteria for denying a request for EHI pursuant to HIPAA or other applicable state laws;
  - Include checklists that workforce members can use to determine whether a patient's signed release of information meets applicable legal requirements (such as a HIPAA authorization checklist);
  - Explain what verification of identity and authority procedures will be followed prior to authorizing access to EHI and why such procedures are in place for purposes of meeting legal preconditions and/or best security practices in the health care industry (see also HIPAA Security Policies); and
  - In cases where workforce members receive a release of information, but conclude that the authorization or consent is not valid, instruct workforce members to use reasonable efforts within their control either to provide the individual with a consent or authorization form that satisfies all required preconditions (such as the organization's release of information form), or provide other reasonable assistance to the individual to satisfy all required elements of the precondition.

## HIPAA Access Policies

The Preventing Harm Safe Harbor is intended to align with a health care provider's existing HIPAA Access Policies. However, in order to qualify for the Preventing Harm Safe Harbor the following updates to an organization's HIPAA Access Policies might be needed:

- ✓ Clarification that the licensed health care professional who makes the individualized determination of harm **must have (or have had) a clinician-patient relationship** with the patient whose EHI will be affected by the determination;

- ✓ Clarification regarding the appropriate harm standard, which will depend on the risk of harm posed and whether it will affect access, exchange or use of EHI by the patient, the patient's legal representative, or someone else; and

- ✓ A requirement that the licensed health care professional document this determination.

Health care providers should also consider expanding these HIPAA Access Policies to document when access, exchange or use of EHI might be delayed or denied under the Preventing Harm Safe Harbor due to corrupted data.

Finally, HIPAA Access Policies should be reviewed to confirm that they align with other potentially applicable Safe Harbors. For example, to qualify for the Fees Safe Harbor with respect to any fees charged in connection with the provision of access, exchange or use of EHI, the following fees **cannot** be charged:

- ✓ Fees prohibited by HIPAA.

- ✓ A fee based in any part on the "electronic access" of an individual's EHI by the individual, the individual's personal representative, or another person or entity designated by the individual. Electronic access means an internet-based method of access that makes EHI available at the time the EHI is requested and where no manual effort is required to fulfill the request (such as through a patient portal).

These excluded fee requirements are just a few of the conditions that must be met to qualify for the Fees Safe Harbor. Many other conditions must also be met, such as basing fees on objective and verifiable criteria that are uniformly applied for all similarly situated classes of persons or entities and requests, and that are reasonably related to the actor's costs. Health care providers thus should also maintain cost records and documentation of the objective criteria for fees charged in connection with providing EHI to defend against allegations of information blocking.

## HIPAA Security Policies

The most salient issue under the Security Safe Harbor is whether an actor's security practices are actually necessary and directly related to addressing a security risk. ONC expects actors to carefully evaluate the risks posed by security threats and develop a considered response that is tailored to mitigating the vulnerabilities of the actor's health IT or other related systems. The best way to accomplish this is to:

- ✓ Complete and maintain an up-to-date security risk analysis (SRA) and risk management plan (RMP), including updating HIPAA Security Policies to incorporate by reference security practices recommended in the RMP for closing gaps identified by the SRA.

- ✓ Update HIPAA Security Policies to include explicit references to specific security standards and health care industry best practices, such as:
  - The security standards set forth in NIST-800-53 Rev. 5, the NIST Cybersecurity Framework, and NIST SP 800-100, SP 800-37 Rev. 2, SP 800-39, as updated and as interpreted through formal guidance; and
  - Best practices developed by bodies such as the International Organization for Standardization (ISO), the Internet Engineering Task Force (IETF), or the International Electrotechnical Commission (IEC).

- ✓ Update HIPAA Security Policies to include objective parameters and time frames for security response plans, such as those set forth in the NIST Incident Response Procedure, US-CERT for interactions with government systems, and ISC-CERT for critical infrastructure.

- ✓ Include within the organization's HIPAA Security Policies a form that captures the necessary Security Safe Harbor documentation elements for security practices that might be needed on a case-by-case basis in direct response to an exigent security incident or threat and that are not otherwise specifically addressed by the HIPAA Security Policies, SRA or RMP.

- ✓ If applicable, address in the HIPAA Security Policies any privacy or security risk notifications or education that will be provided to patients who seek to access, exchange or use their EHI through third party applications.

## HIPAA Administrative Policies

Many of the administrative aspects of information blocking compliance align with HIPAA compliance, such as designating a responsible individual for organizational compliance, workforce training, record retention, reporting and investigating violations, prohibiting retaliation, sanctions for noncompliance, and cooperation with governmental investigations. To reduce administrative compliance burdens, health care providers may leverage their existing HIPAA Administrative Policies to also implement compliance with the Information Blocking Rule.

Additionally, while the Information Blocking Rule does not itemize revisions to be made to HIPAA BAAs, DUAs and other EHI sharing arrangements, the terms and conditions of these agreements might implicate the Information Blocking Rule if they go beyond HIPAA's legal requirements and are used in a discriminatory manner by an actor to forbid or limit disclosures that otherwise would be permitted by HIPAA. Thus, HIPAA

Administrative Policies that address the use of BAAs, DUAs and other EHI sharing arrangements should be reviewed and updated to prohibit the use of such agreements to engage in information blocking. There also may be opportunities to align these HIPAA Administrative Policies with other applicable Safe Harbors—such as the Fees, Licensing and Health IT Performance Safe Harbors—to the extent these agreements are also used to impose fees and other conditions on the use of technology and services to access, exchange or use EHI.

## LEGAL CITATIONS

[1] HIPAA collectively refers to the Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), and their implementing regulations (see 45 C.F.R. Parts 160, 162, and 164), all as amended from time to time.

[2] 45 C.F.R. § 171.201.

[3] 45 C.F.R. § 171.202(b).

[4] 45 C.F.R. § 171.203.

[5] 45 C.F.R. Part 164, Subpart C.

[6] 45 C.F.R. Part 164, Subpart E.