ciitizen

White Paper: HIEs, Info Blocking Rules, & Patient Access

On April 5, 2021, the "information blocking" regulations implementing Section 4004 of the 21st Century Cures Act (the "Cures Act") will go into effect. The intent of these provisions was to counter adverse incentives that undermine the "more connected health system" Congress sought to achieve with its substantial federal investments in health IT infrastructure.[1]

The Cures Act prioritizes access by patients to their medical records from several sources (known as "actors") under the Act. Health Information Exchanges or HIEs (also known as Health Information Networks) are among the three types of "actors" covered by these information blocking rules (referred to here as the "IB Rules"). Starting April 5, 2021, these actors will be obligated to consider record requests from patients - or apps or services engaged by patients – and to provide those records unless an exception applies.

Information blocking is broadly defined as "a practice that, except as *required* by law or specified by the Secretary [in rulemaking], is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information [EHI]." (42 USC 300jj-52(a)(1)(A)) An actor cannot claim that it accidentally "blocked" information that they are required to make available under the HIPAA Privacy Rule. To be subject to a penalty (up to $1 million per violation), HIEs must "know or should know" that a particular act or practice is likely to result in information blocking.[2]

Congress directed ONC to establish exceptions to information blocking. In setting forth these exceptions, ONC defined them narrowly and with some specificity, in order to avoid inadvertently protecting practices that legitimately involve information blocking, while still allowing practices consistent with good public policy.[3]

Patient access to data – either directly or acting through apps or services they engage – is a priority use case under the Cures Act.[4] Today, most HIEs do not share information directly with patients or patient-facing apps or services. However, Congress clearly expects HIEs to assume a new role in actively fulfilling patient access requests. In the Cures Act, Congress directs the HHS Secretary to:

- In coordination with OCR, issue guidance to HIEs on best practices "to ensure that the [EHI] provided to patients is (A) private and secure; (B) accurate; (C) verifiable; and (D) … exchanged" pursuant to a patient's authorization where one is required by law. (42 USC 300jj-19(c)(3)).

[1] 85 Fed. Reg. 25642, at 25790 (May 1, 2020).

[2] 42 USC 300jj-52(a)(1)(B)(i)).

[3] 85 Fed. Reg. 25642, at 25791 & 25809 (May 1, 2020).

[4] 85 Fed. Reg. 25642 at 25810 (May 1, 2020).

- Use "existing authorities to encourage partnerships between [HIEs] and health care providers, health plans, and other appropriate entities with the goal of offering patients access to their [EHI] in a single longitudinal format that is easy to understand, secure, and may be updated automatically"). (42 USC 300jj-19(c)(1))

- In coordination with OCR, "educate health care providers on ways of leveraging the capabilities of [HIEs] (or other relevant platforms) to provide patients with access to their [EHI]" and "clarify misunderstandings by health care providers about using [HIEs] (or other relevant platforms) for patient access to [EHI]." (42 USC 300jj-19(c)(2)(A)&(B))

- In consultation with ONC, promote policies that "ensure that a patient's [EHI] is accessible to that patient and the patient's designees, in a manner that facilitates communication with the patient's health care providers and other individuals, including researchers, consistent with such patient's consent" and promote awareness of the patient's right to access PHI under HIPAA. (42 USC 300jj-19(e)(1)(A)&(B)).

Section 4006 also requires ONC and OCR to "jointly promote patient access to health information in a manner that would ensure that such information is available in a form convenient for the patient, in a reasonable manner, without burdening the health care provider involved."[5] (42 USC 300jj-19(d))

ONC recognized the priority the Cures Act placed on the patient access use case. In guidance issued with the final IB Rules, ONC stated that information blocking "will almost always be implicated when a practice interferes with access, exchange, or use of EHI for certain purposes, including…[p]roviding patients with access to their EHI and the ability to exchange and use it without special effort." (85 Fed. Reg. 25642 at 25810 (May 1, 2020)).

These IB Rules were published as final on May 1, 2020 – and the effective date has already been pushed back once to allow actors more time to get ready to comply. It is unlikely the effective date will be pushed back beyond April 5, 2021, already almost a year after the rules were finalized and more than two years since they were initially proposed. In response to unprecedented demands that COVID-19 has placed on actors (and the lack of final enforcement regulations from OIG), it is likely that enforcement by OIG and CMS may not ramp up to full issuance of penalties (and disincentive or false claims actions) for another 6-12 months (or longer).

Many in the HIE and wider health IT community have questions about the requirements under the IB Rules for HIEs to fulfill patient access requests, and in particular whether existing restrictions in BAAs between HIEs and other IB actors may excuse HIEs from fulfilling these requests. We believe clear guidance from the ONC and OCR is needed soon, to give HIEs and

[5] Of note, Section 4003 also establishes individual access to electronic health information as a priority for the new HIT Advisory Committee.

other actors adequate time to prepare for compliance. We hope this legal analysis (and the powerpoint deck accompanying it) helps in that effort. **Ciitizen is eager to work with HIEs to facilitate compliance with the IB Rules with respect to patient access.**

Coverage of HIEs by the IB Rules.

The Act lists three types of entities that are required to comply with the IB Rules: health care providers, certified health information technology vendors, and health information networks and health information exchanges (HIN/HIEs).[6] (42 USC 300jj-52(a)(1)(B)) The regulatory definition makes it clear that traditional HIEs facilitating the exchange of data among participants for treatment, payment, and operations (TPO) are covered by these rules.

Specifically, an HIE is:

> an individual or entity that determines, controls, or has the discretion to administer any requirement, policy, or agreement that permits, enables, or requires the use of any technology or services for access, exchange, or use of EHI:
> - Among more than two unaffiliated individuals or entities [not the HIE] that are enabled to exchange with each other; and
> - That is for a treatment, payment or health care operations purpose [as defined in HIPAA], regardless of whether such individuals or entities are subject to [HIPAA]. (42 CFR 171.102)

As HIEs are explicitly called out in the Act, all of its practices are subject to the IB Rules, not just those involving the exchange of information for treatment, patient, operations (TPO). (85 Fed. Reg. 25642 at 25802 (May 1, 2020)) Failing to share information risks an IB Rule violation unless the rationale for not sharing fits in one of the eight exceptions.

Certified Health Information Technology vendors that also facilitate health information exchange for TPO among two or more unaffiliated customers arguably meet the definition of HIE and are therefore covered as both vendors and HIEs under the information blocking rules.[7]

HIE Obligations to Directly Comply With IB Rules

HIEs (and other IB actors) are independently responsible for directly responding to information requests under the Act. A response that directs requestors to get information instead from

[6] The Cures Act did not attempt to define an HIN or an HIE; instead, ONC combined the two and established a single "functional" definition of HIE or HIN. 45 C.F.R. §171.102. In this discussion, when we refer to HIEs, we mean HIEs or HINs.

[7] In guidance, ONC provides an example of a healthcare provider that has an ownership interest in an HIE but denies an individual access to EHI through the provider's EHR portal. In this situation, the provider is potentially "blocking" information in its role as a provider, not as an HIE. So ONC expressly acknowledges that actors may provide a myriad of functions - and that their obligations under the information blocking rules could depend which role/function was involved in the alleged blocking activity. 85 Fed. Reg. 25642, at 25803 (May 1, 2020).

health care providers risks an IB Rules violation. Of particular concern for ONC in establishing the IB Rules were practices that impeded the use of technologies (such as HIE/HIN) upon which entities depend for the exchange of EHI (i.e., interoperability elements). (85 Fed. Reg. 25642, at 25810 (May 1, 2020))

There is guidance from ONC regarding the separate EHR certification rules allowing certified EHR technology vendors – when acting in their roles as certified technology vendors – to allow their customers (health care providers) to decide which apps and services with which to connect (subject to the *provider's* IB rule obligations). (85 Fed. Reg. 25642, at 25745 & 25748 (May 1, 2020)) But notably, this interpretation is not part of the IB Rules, which are separate from the certification rules. There is nothing in the IB Rules or existing guidance that suggests an actor can comply with the IB rules by sending the patient to alternative data sources for EHI held by that actor.

Contrary BAA Provisions or HIE Policies

ONC's existing guidance on whether contractual provisions or pre-existing policies meet the "infeasibility" exception is somewhat conflicting and incomplete.

On one hand, ONC addressed whether the IB Rules would require actors to potentially violate their business associate agreements and responded as follows: "While the information blocking rule does not require actors to violate these agreements, a BAA or its associated service level agreements must not be used in a discriminatory manner by an actor to forbid or limit disclosures that otherwise would be permitted by the Privacy Rule." The example provided by ONC involves an actor refusing to share EHI with one provider for treatment purposes, while enabling sharing of EHI with other providers for treatment purposes. (https://www.healthit.gov/curesrule/resources/information-blocking-faqs) The example did not directly address whether actors could – in BAAs – limit the purposes for which they would share EHI and rely on those contractual provisions to block information sharing for any purpose other than what is permitted by the BAA.

But other provisions in ONC's guidance clearly state that actors cannot – by contract or by policy – limit the purposes for which they share information and rely on those voluntarily-adopted limitations in claiming that sharing of information is "infeasible:"

- An "actor's organizational policies and procedures should not be used as a pretext for information blocking." (85 Fed. Reg. 25642, at 25850 (May 1, 2020))

- "We do not agree that health information exchanges or networks should be given a blanket exemption based on their existing written governance policies because that could lead to a situation involving information blocking if those policies imposed conditions that conflict with the information blocking provision." (85 Fed. Reg. 25642, at 25850 (May 1, 2020))

- ”If a [HIN/HIE] was exchanging EHI on behalf of a health care provider for treatment purposes but denied an individual access to their EHI available in the [HIE/HIN], then the [HIE/HIN] would be considered [an HIE/HIN] under the circumstances for purposes of information blocking.” (However, ONC followed this sentence by stating: “Having said this, the HIN/HIE may not have ‘interfered with’ the individual’s access to their EHI depending on the terms of the HIN/HIE’s business associate agreements with the participating covered entities…”) (85 Fed. Reg. 25642, at 25802 (May 1, 2020))

- “If an actor is permitted to provide access, exchange, or use of EHI under the HIPAA Privacy Rule (or any other law), then the information blocking provision would require that the actor provide that access, exchange, or use of EHI so long as the actor is not prohibited by law from doing so (assuming that no exception is available to the actor).” (85 Fed. Reg. 25642, at 25812 (May 1, 2020))

ONC also recently issued a new FAQ making clear that prior agreements or policies can implicate the IB rules, so the fact that these agreements or policies pre-dated the IB rules does not provide a valid excuse for not responding to an information request.[8] More broadly, to allow actors to use a BAA to significantly limit information sharing would completely undermine the intent of Congress when it drafted the Act. As noted above, Section 4006 - which follows the information blocking provisions (Section 4004) obligating HIEs to share data - specifically mentions HIEs providing EHI to patients.

And there is potential for some additional confusion. In a separate provision of the Cures Act, Congress provided that “business associates” could voluntarily adopt to provide patients with access to their health information pursuant to the HIPAA Right of Access. (Cures Act Section 4006(b)) However, in Section 4004 Congress also singled out HIEs/HINs and certified technology vendors and placed heightened expectations on those entities for interoperability of health information, including for exchange of data with patients. Reading Section 4004 (Information Blocking) together with Section 4006 (expressly calling out HIEs in providing data to patients), Congress intended to obligate HIEs to provide information to patients but also allow business associates not subject to the IB Rules discretion as to whether to provide information directly to patients.

Of note, undue reliance on BAA provisions as a rationale for declining to share EHI with patients may subject all parties to the BAA who are “actors” to potential penalties (or adverse action from CMS on the part of providers). In guidance, ONC stated further, “To be clear, both the health care provider(s) who initiated the BAA and the BA who may be an actor…would be subject to the information blocking provision[s]….” (85 Fed. Reg. 25642, at 25812 (May 1, 2020))

[8] https://www.healthit.gov/curesrule/resources/information-blocking-faqs.

Relationship Between BAAs and IB Rules Compliance

Guidance from ONC and OCR should make clear that HIEs/HINs need not be concerned about whether violating their business associate agreements risks a HIPAA violation and potential penalties. It is clear that there is no HIPAA violation when a business associate discloses EHI where required by law to do so - and the Cures Act establishes a separate legal obligation to share EHI. The HIPAA Privacy Rule provides that business associates may use or disclose protected health information (PHI) (of which EHI is a subset) only as permitted by their BAA "or as required by law." (45 CFR 164.502(a)(3)) The Privacy Rule also requires BAs to make data available to patients. For example, the Rule states that BAAs must include provisions requiring the business associate to "make PHI available in accordance with" the HIPAA individual right of access provisions (45 CFR 164.504(e)(2)), and business associates are required to disclose PHI "to a covered entity, the individual or the individual's designee." (45 CFR 164.502(a)(4)(ii)) Although in pre-existing guidance OCR has urged covered entities and business associates to establish in the BAA which entity is responsible for responding to an individual's right of access request,[9] the regulations clearly obligate business associates to make PHI available to individuals and envision that this information could be provided directly. This guidance needs to be updated in light of provisions of the Cures Act designating two types of business associates (HIEs and certified EHR vendors) as directly accountable for responding to patient access requests.

Bottom line: Given that the HIPAA regulations expressly contemplate business associates responding to individual access requests, and the Act and associated IB Rules require a response to such requests, HIEs likely will not be able to claim infeasibility due to contractually imposed (BAA) barriers.

Further, in the past when law changes have resulted in the need for BAAs to be updated, OCR has customarily allowed covered entities and business associates some time to amend BAAs to catch up to changes in the law.[10]

Concerns about Identity Proofing

It is unlikely that HIE concerns about identity proofing patients would rise to the level of a blanket exemption for providing patient access. HIEs have an obligation as business associates under the HIPAA Security Rule to have a process for assuring the identity of a patient requesting their information. This will not be easy for HIEs, most of which do not have relationships with individuals. Such identity proofing will need to take place entirely remotely, and it is likely HIEs will want to reasonably rely on the identity proofing practices of an individual's app or service if such reliance is reasonable. There is no one particular way to do

[9] For example, see 78 Fed Reg. 5566 at 5599 (January 25, 2013) (the Omnibus Rule).

[10] See, for example, discussion in the Omnibus Rule (78 Fed. Reg. 5566 at 5602-03 (January 25, 2013).

remote ID proofing, and best practices are still emerging. However, it is critical that HIEs not set identity proofing requirements so high that it is difficult for individuals (or their apps and services) to meet those requirements, as those requirements could be found to be information blocking. The goal is risk reduction, not risk elimination. As ONC stated in guidance: "If an actor chooses not to provide access, exchange, or use of EHI on the basis that the actor's identity verification requirements have not been satisfied, the actor's practice must be tailored to the specific privacy risks at issue…..[T]his would require that the actor ensure that it does not impose identity verification requirements that are unreasonably onerous under the circumstances." (85 Fed. Reg. 25642, at 25850 (May 1, 2020)) **Ciitizen can assist HIEs by identity proofing patients seeking access to records using processes intended to comply with NIST standards for remote identity proofing (level of assurance 2)**.

Concerns about Privacy and Security of Apps Chosen by Individuals

ONC's existing guidance has been clear that concerns about the privacy and security of tools used by patients to access and store their EHI may not be used as an excuse for declining to share EHI – but additional guidance reinforcing this point could be helpful. (85 Fed. Reg. 247642, at 25814-17 (May 1, 2020)) Actors are permitted to educate patients about the privacy and security practices of apps and other parties with whom a patient might share their EHI; however, such education must:

- Focus on any "current privacy and/or security risks" posed by the app or app developer;
- Be "factually accurate, unbiased, objective, and not unfair or deceptive;" and
- Be provided in a nondiscriminatory manner. (85 Fed. Reg. 24642, at 25815 (May 1, 2020)

However, "an actor may not prevent an individual from deciding to provide its EHI to a technology developer or app despite any risks noted regarding the app itself or the third-party developer." (Id.) **Ciitizen has attested to the CARIN Code of Conduct and does not share a patient's data with third parties without the patient's consent.**

Adoption of New Technology

As we read current guidance, HIEs are not required to establish portals or adopt FHIR APIs in order to comply with the IB Rules. ONC's more recent guidance has made clear that adoption of certified technology is not required by the IB Rules; however, additional guidance on this point could be helpful. If the requested manner for sharing EHI is not "technically feasible" or the actor cannot reach agreeable terms with the requestor (in this case, the patient or the app or service acting on the patient's behalf) for how to fulfill the request, the actor is allowed to fulfill the request for EHI in an alternative manner. (85 Fed. Reg. 25642, at 25877[11]; 45 CFR

[11] Here ONC provides an example of an individual requesting their EHI via an API in a circumstance where an actor cannot fulfill the request via API; the individual requested e-mail as an alternative, and the actor granted the request in that manner.

171.301(b)(1)(i)) The IB rules establish a priority order for alternative mechanisms for providing EHI - but the viability of each option depends on whether it is technically feasible for the actor to produce the EHI using this mechanism:

1. Using technology certified to standards set by ONC for certified EHR technology that are specified by the requestor;
2. Using content and transport standards specified by the requestor and published by the federal government, or a standards developing organization accredited by the American National Standards Institute; or
3. Using an alternative machine readable format, including the means to interpret the electronic health information , agreed upon with the requestor. (Id.)

Guidance could urge HIEs to consider how their current processes for exchange of EHI among participants can be opened to allow individuals (or apps or services working on their behalf) to obtain EHI, as this may be the most convenient mechanism for both the HIE and the requestor. **Ciitizen will work with HIEs to leverage technology used by or familiar to HIEs to facilitate patient access.**

Questions? Need Help? Please contact Deven McGraw, Chief Regulatory Officer of Ciitizen, at deven@ciitizen.com.