PREPARE NOW FOR SHARING OF AND ACCESS TO ELECTRONIC HEALTH INFORMATION: CURES ACT INFORMATION BLOCKING AND INTEROPERABILITY RULES TAKE EFFECT JUNE 30, 2020

AUTHOR(S) Amy S. Leopard, Jordan Luke, Elliot Bertasi

The U.S. Department of Health and Human Services (HHS) companion regulations advancing the interoperability of and patient access to electronic health information under the 21st Century Cures Act take effect June 30, 2020, with a compliance date of November 2, 2020. HHS agencies coordinated on the timing, compliance priorities, and enforcement approach they will take to implement the Cures Act goals of creating an interoperable health system that shares electronic health information (EHI) when and where needed.

The HHS Office of the National Coordinator for Health IT (ONC) finalized its rule limiting information blocking practices of certain actors (the "Information Blocking Rule"). The final rule from the Centers for Medicare and Medicaid Services (CMS) places new responsibilities on hospitals and the health plans that CMS regulates to require broader data sharing between them and the electronic delivery of health information to patients (the "CMS Interoperability and Patient Access Rules").

The final publication of these rules on May 1, 2020, follows the April 24, 2020, HHS Office of Inspector General (OIG) proposal for analyzing information blocking claims and outlining its civil monetary penalty (CMP) enforcement approach. Owing to the novel coronavirus (COVID-19) public health emergency, HHS extended the compliance date and established enforcement discretion beyond the compliance date. The agencies have promised not to subject information blocking practices occurring before OIG finalizes the information blocking CMP, and the OIG expects to grant a 60-day enforcement delay in its final rule.

The HHS rules are transformative, intended to advance the digital age of health information sharing. The information blocking and interoperability rules are also dense and technical and impact many internal and external stakeholders. Now is the time to learn what these rules will require and begin the work with stakeholders to establish new practices for advancing interoperability goals safely and securely.

THE INFORMATION BLOCKING RULE – NOVEMBER 2, 2020 COMPLIANCE DATE

Section 4004 of the Cures Act defines "information blocking" as a practice by a health care provider, health IT developer, or health information network or exchange that is unreasonable and likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI. The Cures Act authorized HHS to identify certain practices that technically meet the definition of information blocking but are reasonable and necessary to further the underlying data sharing goals of the Cures Act, a task that HHS delegated to ONC.

The centerpiece of the ONC rule includes the final exceptions to the information blocking provisions of the Cures Act governing how technology is used to share EHI, a term not defined in the Cures Act. ONC and OIG clarified that the OIG will assess the facts and circumstances of an information blocking claim on a case-by-case basis to determine whether the conduct meets the definition of information blocking and is not required by law, the actor's requisite level of intent, and whether an exception is met.

ACTORS, PRACTICES, AND INFORMATION REGULATED

The Information Blocking Rule governs providers, health IT developers, and health information networks and exchanges (referred to as "actors"). ***Health care provider*** is a broad term encompassing a long list of provider types, each of whom are regulated without regard to whether they are covered entities under HIPAA. ONC will regulate ***health IT developers*** who develop or offer health information technology that at the time of the information blocking practice, has one or more modules certified under ONC's Health IT Certification program. The definition excludes healthcare providers that self-develop health IT for their own internal use, but not when they offer certified health IT for other entities to use in their own independent operations.

INITIAL STEPS

With the upcoming compliance dates, here are some initial steps for health care organizations and health IT developers to get started:

2020 Action Plan for Information Blocking

1. Educate leaders and core operational staff and vendors (privacy, security, HIM, IT, release of information, finance, legal) on Information Blocking Rule concepts and operational details.
2. Update privacy and information security policies and procedures for required data sharing consistent with HIPAA, CARES Act Part 2 changes, and state law.
3. Consider opportunities to leverage USCDI elements as a default safe harbor.
4. Review material data and technology licensing terms for interoperability elements for compliance with the Information Blocking Fee, Licensing, or Content and Manner Exceptions and confirm SLAs for Health IT Performance Exception.
5. Adopt API policy and third-party app security protocol.
6. Update procedures and communications for patient access, required consents, right-to-request restrictions, and third-party app security profiles.
7. Update identity and authority verification for third-party access and disclosures.
8. Update BAA security provisions to tailor risk and avoid individual determinations.
9. Participate in industry coalitions to standardize terms.
10. Update security risk assessment to address environmental and operational impacts of Information Blocking Rule and response.

ONC consolidated the Cures Act definitions of ***health information networks (HINs) and health information exchanges (HIEs)*** given the overlap between the two categories of actors. Health information networks and exchanges subject to information blocking claims are those that determine, control, or have 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 (other than the actor to which the definition applies). Importantly, ONC has limited the scope of the definition to health information networks and exchanges enabled to exchange for treatment, payment or health care operations purposes under HIPAA (even if the actor is not subject to HIPAA as a covered entity or business associate). That limitation excludes health information networks and exchanges engaged for research or public health reporting and portals for patients and family members.

ONC outlines five types of practices that serve as examples of conduct that may be likely to interfere with the access, exchange or use of EHI as follows:

- Imposing restrictions on the access, exchange, or use of EHI
- Imposing limits or restrictions on the interoperability of health IT
- Impeding innovation and advancements in access, exchange or use of health IT-enabled care delivery
- Rent seeking and opportunistic pricing practices
- Non-standard implementation practices that lead to unnecessary complexity and burden

In the Information Blocking Rule, ONC narrowed the scope of EHI to electronic protected health information (ePHI) as defined under HIPAA to the extent that it would be included in a designated record set (also as defined under HIPAA), with certain exclusions, regardless of whether the health information is held by a HIPAA-covered entity.

INFORMATION BLOCKING EXCEPTIONS

ONC had proposed that, in the event of an investigation of an information blocking complaint, an actor must demonstrate that an exception to an information blocking practice is applicable and that the actor met all relevant conditions of the exception at all relevant times for each practice for which it sought an exception. ONC received more than 2,000 comments, many seeking clarification regarding the type and amount of documentation required for an actor to demonstrate compliance, stemming from a concern that meeting the exceptions would substantially increase documentation burden and other administrative costs.

In response, ONC finalized eight categories of reasonable and necessary practices that will not be considered information blocking. ONC narrowed and tailored the exceptions and provided more detail to explain what an actor must do to meet each exception, including the conditions that must be met for the activity to be exempt. Often this includes a writing or documentation requirement to demonstrate that the practice meets all the conditions of the exception.

ONC emphasized that failure to meet an exception does not necessarily mean a practice meets the definition of information blocking. As such, the exceptions operate much like the safe harbors under the federal Anti-Kickback Statute, requiring that the facts and circumstances surrounding information blocking claims be analyzed on a case-by-case basis. Outside the exceptions, the OIG will investigate practices that implicate the information blocking prohibition to determine whether the practice rises to the level of an interference and whether the actor acted with the requisite intent. ONC encouraged actors to voluntarily comply with an exception so that their practices are not subject to information blocking investigations.

ONC divided the exceptions into two categories: those exceptions for requests to access, exchange or use EHI that are not fulfilled, and those exceptions governing how requests to access, exchange or use EHI would be fulfilled.

EXCEPTIONS THAT INVOLVE NOT FULFILLING REQUESTS TO ACCESS, EXCHANGE, OR USE EHI

1. **Privacy Exception – When will an actor's practice of not fulfilling a request to access, exchange, or use EHI in order to protect an individual's privacy not be considered information blocking?**

   An actor may decline to fulfill a request to access, exchange, or use EHI in order to protect an individual's privacy, provided certain conditions are met. ONC created four privacy sub-exceptions that permit an actor to deny requests on the grounds of protecting individual privacy:

   - For actors required to satisfy preconditions required by federal or state privacy laws (e.g., consent) when that precondition has not been satisfied, provided the actor uses reasonable efforts within its control to provide the individual with a consent or authorization form satisfying all applicable requirements or provide other reasonable assistance with respect to deficiencies. The final Privacy Exception moves some of the burden to the individual to provide consent.
   - For covered entities and their business associates, following the applicable provisions in the HIPAA Privacy Rule for the unreviewable grounds of a denial of the individual's access request.
   - For health IT developers not regulated by HIPAA, under their privacy policies if certain conditions are met.
   - For requested restrictions from an individual not to provide access, exchange or use of EHI, provided certain conditions are met.

2. **Security Exception – When will an actor's practice that is likely to interfere with the access, exchange, or use of EHI in order to protect the security of EHI not be considered information blocking?**

   It is not information blocking for an actor to interfere with the access, exchange, or use of EHI to protect the security of EHI, provided certain conditions are met. A key condition of the exception is that the practice must either implement a qualifying security policy or security determination and be:

   - Directly related to safeguarding the confidentiality, integrity, and availability of EHI;
   - Tailored to the specific security risks; and
   - Implemented in a consistent and non-discriminatory manner.

   The Security Exception requires actors to adopt a written organizational security policy that follows the HIPAA Security Standards and consensus-based standards such as NIST. Otherwise, the facts and circumstances surrounding the practice will be analyzed under a stricter standard to determine whether the practice is necessary to mitigate the security risk to EHI, and there are no reasonable and appropriate alternatives to the practice.

3. **Preventing Harms Exception – When will an actor's practice that is likely to interfere with the access, exchange, or use of EHI in order to prevent harm not be considered information blocking?**

   ONC heard comments from providers that this exception should be aligned with the HIPAA rules permitting the denial of an individual access request for their own health information when a licensed healthcare professional determines that certain harms may occur. Under the Preventing Harm Exception, it is not information blocking for an actor to engage in practices that are reasonable and necessary to prevent harm to a patient or another person, provided certain conditions are met, including:

   - The actor reasonably believes the practice will substantially reduce a risk of harm;
   - The practice is no broader than necessary;
   - The practice satisfies at least one condition from each of the following categories: type of risk, type of harm, and implementation basis; and
   - The practice gives patients the right to request review of an individualized determination of risk of harm.

4. **Infeasibility Exception – When will an actor's practice of not fulfilling a request to access, exchange, or use EHI due to the infeasibility of the request not be considered information blocking?**

   It is not information blocking if an actor does not fulfill a request to access, exchange, or use EHI due to the request being infeasible, defined to include the following events:

   - Uncontrollable events, enumerated to include such events as public health emergencies, internet service disruption, and regulatory acts;
   - The inability to unambiguously segment the requested EHI from EHI that cannot be disclosed due to legal restrictions or the individual's preference; and
   - The actor demonstrates with contemporaneous records that it considered the request infeasible under several factors in a consistent and nondiscriminatory fashion.

   The Infeasibility Exception requires an actor to provide a written response to the requestor within ten (10) business days of receipt of the request with the reason(s) why the request is infeasible.

5. **Health IT Performance Exception – When will an actor's practice that is implemented to maintain or improve health IT performance and that is likely to interfere with the access, exchange, or use of EHI not be considered information blocking?**

   It is not information blocking for an actor to take 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 the health IT, provided certain conditions are met. The Health IT Performance Exception requires that the practice last no longer than necessary and establishes conditions under four different sub-exceptions for maintenance and improvement to health IT, assuring a level of performance when third-party apps impact performance, responding to a risk of harm to a patient or another person subject to the Risk of Harm Exception, and security-related practices subject to the Security Exception.

EXCEPTIONS INVOLVING THE PROCEDURES FOR FULFILLING REQUESTS TO ACCESS, EXCHANGE, OR USE EHI

1. **Content and Manner Exception – When will an actor's practice of limiting the content of its response or the manner in which it fulfills a request to access, exchange, or use EHI not be considered information blocking?**

ONC finalized the Content and Manner Exception to address concerns with the scope and manner of EHI that actors would need to provide in all circumstances when fulfilling requests. It is not information blocking for an actor to limit the content or manner when fulfilling a request for the access, exchange or use of EHI by meeting both conditions.

- Content: Until May 2, 2022, an actor may limit the content of the EHI that fulfills a request to access, exchange or use EHI to the data elements listed in the U.S. Core Data for Interoperability (USCDI) standard and the limit will not be considered information blocking. On or after that date, an actor must respond to the request with the full scope of data in the EHI definition above.
- Manner: The actor must fulfill the request in the manner requested unless technically unable to do so or the actor and the requestor mutually agree on license terms. If the parties cannot agree on terms, the actor must fulfill the request in an alternative manner based on an order of priority specified by rule, namely, first by using ONC-certified health IT, then federal or ANSI-accredited standards-based content and transport standards that the requestor specified, or finally through a machine-readable format capable of interpreting the data agreed to by the parties.

2. **Reasonable Fees Exception – When will an actor's practice of charging fees for accessing, exchanging, or using EHI not be considered information blocking?**

   Under the Reasonable Fees Exception, it is not information blocking for an actor to charge fees that result in a reasonable profit margin for accessing, exchanging, or using EHI provided certain conditions are met. The exception excludes certain fees and requires that the permissible fees meet uniformly applied objective criteria, be reasonably related to costs not already recovered, and be determined based on a reasonable allocation of costs. Health IT developers must comply with the ONC standards for API technology and further limit fees to healthcare providers and third-party application developers.

3. **Licensing Exception – When will an actor's practice to license interoperability elements for EHI to be accessed, exchanged, or used not be considered information blocking?**

   It is not information blocking for an actor to refrain from licensing certain of its interoperability elements it controls, such as intellectual property rights, hardware, software, technologies, or services, when the actor fulfills a request for EHI to be accessed, exchanged, or used in an alternative manner. The actor must initiate negotiations with the requestor on the terms for licensing the interoperability elements within 10 business days of receiving the request and finalize the negotiations within 30 business days of receiving the request. Those licensing terms and any royalty must be reasonable and non-discriminatory and meet enumerated conditions under the Licensing Exception.

CMS FINAL INTEROPERABILITY AND PATIENT ACCESS RULE

The CMS Interoperability and Patient Access Rule is effective June 30, 2020, with varying compliance deadlines and COVID-19 extensions as follows:

HOSPITAL CONDITIONS OF PARTICIPATION (COPS) REQUIRE ELECTRONIC PATIENT EVENT NOTIFICATIONS

CMS is modifying the COPs to require hospitals, including CAHs and psychiatric hospitals, to send electronic patient event notifications upon a patient's admission, discharge, and/or transfer (ADT notifications). CMS sees these requirements as supporting both the Information Blocking Rule and the Hospital Discharge Planning Rule finalized in September 2019.

Effective May 2, 2021, these requirements only apply to those hospitals that currently possess EHR systems with the technical capacity to generate the required information (e.g., all hospitals using certified EHR). Hospitals must provide ADT notifications, at minimum, for inpatients admitted to, discharged, and/or transferred from the hospital to the applicable primary care practitioner and post-acute care providers and suppliers to whom a patient is being transferred or referred. CMS adopts a "reasonable effort" standard to ensure hospitals collect the information to notify the specified providers.

At this point, no specific standard is required to format or deliver ADT notifications, since the functionality for these notifications are not currently certified by ONC. CMS notes that low-cost solutions are available and permits hospitals to use intermediaries such as health information networks to deliver the notifications to external providers. Until consensus standards develop, CMS will require, at a minimum, that patient health information in the ADT notification include patient name, treating practitioner name, and sending institution name. The patient diagnosis is not required but is strongly recommended if not prohibited by other applicable law.

CMS encourages hospitals and other providers and practitioners to utilize ADT notifications to coordinate care and appropriate follow-up care in a wider range of patient situations.

PATIENT ACCESS TO HEALTH PLAN INFORMATION VIA STANDARDS APIS

Beginning January 1, 2021, CMS will require Medicare Advantage (MA) organizations, state Medicaid agencies, Medicaid managed care plans, Children's Health Insurance Program (CHIP) agencies, CHIP managed care plans, and Qualified Health Plan (QHP) issuers on the Federally Facilitated Exchanges (FFEs) (CMS-regulated payers), with certain exceptions noted below, to implement and maintain standards-based APIs. API technologies permit third-party software or applications to retrieve, on behalf and at the direction of the patient (or the patient's representative), certain clinical and payment information that CMS-regulated payers hold. Patients must be able to access APIs using their common electronic devices, excluding QHP issuers on the FFEs offering only stand-alone dental plans and those only offering QHPs in the federally facilitated Small Business Health Options Program Exchanges.

By January 1, 2021, the data from patient services occurring on or after January 1, 2016, must be available on the patient access API. At a minimum, the scope of the data that must be available for patient access from the API is: (1) adjudicated claims (including provider remittances and enrollee cost-sharing); (2) encounters with capitated providers; and (3) clinical data, including clinical laboratory results maintained by the payer. The data must be available for patient access on the payer's API within one (1) business day of the payer receiving the data.

The proposed rule considered requiring the applicable payers to make provider directory information and certain pharmacy directory and formulary data (in the case of MA Part D plans) available in the patient access API. Beginning January 1, 2021, CMS-regulated payers (except for QHP issuers on the FFEs) must make accessible both the provider directory information and such pharmacy benefit data (in the case of MA Part D plans) in a separate public-facing provider directory API.

Each CMS-regulated payer not only must bear the cost of implementing patient access APIs, but also routinely test and monitor its APIs. Testing and monitoring are essential for maintaining privacy and security. Each CMS-regulated payer must take appropriate measures to ensure individual patients and their representatives can only access the data or other PHI that belongs to that patient.

Finally, CMS-regulated payers implementing and maintaining APIs also must make available to enrollees' certain information to assist the enrollees in selecting an application to access the API. This assistance should include practical strategies for safeguarding their privacy and security, as well as mechanisms for submitting complaints to OCR or FTC. CMS is providing suggested resources and content for this requirement.

COORDINATION OF CARE – HEALTH INFORMATION EXCHANGE AND TRUST EXCHANGE NETWORK (PLANS)

By January 1, 2022, MA organizations, Medicaid managed care plans, CHIP managed care plans, and QHP issuers on the FFEs must send certain patient information to another payer as directed by and with the approval of the patient. That patient information is only required to be sent in the electronic form and format in which it was received for up to five years of patient records, if available.

The proposed rule considered requiring applicable healthcare plans to participate in a trusted exchange network to advance interoperability. Due to the possibility of leveraging existing trust networks (e.g., ONC's Trusted Exchange Framework and Common Agreement (TEFCA)) that have not yet been finalized, CMS has not yet finalized a proposal, but instead is monitoring existing networks to inform possible future participation in a trusted exchange network.

TAKEAWAYS

CONTROVERSIES, OPPORTUNITIES AND TURNING HIPAA (POLICIES AND PROCEDURES) UPSIDE DOWN

The Information Blocking Rule in particular has been laden with controversy. Various industry players have sought to delay or cull the data liquidity provisions, often citing the privacy and security risks of moving data protected by HIPAA to other repositories that are not regulated.

When an actor is permitted to provide access, exchange or use of ePHI under HIPAA, the Information Blocking Rule requires the actor to do so unless prohibited by law or an exception is met. In essence, the Information Blocking Rule will turn HIPAA on its head by requiring healthcare providers and their business associates to share data in instances where HIPAA permits the disclosure and their existing practices prohibit or delay that data sharing. This sea change in the regulatory landscape will require covered entities and their business associates to dust off their privacy and security policies and reconsider and modify their release of information and data-sharing practices under the Information Blocking Rules. If delay or denial of information may be considered interference, compliance with an exception may be necessary to avoid information blocking claims. Finding the right balance between uniformity to support nondiscriminatory practices and tailoring procedures to specific privacy and security risks will likely be very challenging.

Likewise, extensive concerns that actors are losing their trade secret investments in proprietary interoperability elements are now in the distant past as the train prepares to leave the station. Despite those risks, there are other stakeholders and market entrants embracing this data liquidity and building business models designed to capture and capitalize on data exchange. ONC has finalized requirements for health IT developers to adopt standards for their certified health IT products that will assist providers with sharing EHI with patients via apps and exporting single or multiple patient data for analytics or EHR conversions. Health IT developers will be updating their products to meet standard certification criteria for standards-based application programming interfaces (standard API), beginning with the HL7® FHIR Release 4 as an initial foundational standard. Next up will be the standard EHI data export capabilities that allow providers to export one or all of their medical records to a new platform or repository.

All actors will need to brace themselves for an onslaught of requests for electronic health information, particularly via third-party app developers using the API interfaces to transmit a patient's health information to their smartphone for use with their app. Focusing on giving patient access requests immediate priority seems a good compliance strategy for most actors, but ONC permits some diligence and even patient education on privacy and security considerations. ONC states that actors may bring to the attention of patients whether the third-party app developer receiving their EHI can attest to having privacy and security policies and practices that meet industry standards without triggering information blocking claims. This patient education could occur through written notice or pointing out or displaying in advance this deficiency as part of the app authorization process.

IMPACT ON DATA SHARING AND TECHNOLOGY CONTRACTING

The Information Blocking Rule will place pressure on all actors to streamline their technology and data contracting protocols for technology tools and data sharing projects involving EHI. In both cases, clear understanding of how the data flows and the purposes of the disclosure will help the entities determine whether interference is likely, non-disclosure is required by law, and which exception will provide the most immediate relief from an information blocking

claim. For hospitals, sending patient event notifications to coordinate care and appropriate follow up with other providers will become routine. The CMS Interoperability and Patient Access Rule will be a strong driver for data sharing across the continuum of care when a hospital is involved.

Under the Information Blocking Rule, ONC alludes to the potential for information blocking claims to arise when a provider leaves a practice and the sharing of EHI is not handled appropriately. Data-sharing projects will be particularly reliant on the Content and Manner Exception to fulfill data requests, certainly from patients and third parties acting on their behalf as well as the actor's competitors. Actors will find that having the ability to transmit the USCDI data elements will be at a premium to take advantage of this useful exception.

To the extent the negotiation strategy instead requires reliance on the Licensing or Fee Exceptions, reasonable licensing terms and allowable fees will need to be considered, as well as timeframes for negotiating license conditions on non-discriminatory terms. HIPAA historically required business associate agreements to establish permissible uses and disclosures of PHI and to prohibit uses and disclosures not permitted or required by law. Now, when the law permits the access to or exchange of EHI, disclosure often will be required unless an exception is met. Although ONC notes that the Information Blocking Rule does not itself require actors to violate their business associate agreements and associated service level agreements, actors cannot use these agreements to limit EHI disclosures in an arbitrary manner.

COMPLIANCE TIMEFRAMES AND ENFORCEMENT APPROACH

The three agencies have aligned their regulatory authorities for compliance and enforcement. ONC has developed a portal through which anyone may file an information blocking complaint against an actor. The OIG will use its CMP authority to take the lead on enforcement and determine whether CMPs apply to health IT developers and health information exchanges that possess the requisite level of intent for practices that meet the definition of information blocking, are not required by law, and where an information blocking exception is not met. Under the Cures Act, the OIG may levy CMPs up to $1 million per violation against health IT developers and health information networks and exchanges that knew or should know the practice constitutes information blocking. The OIG has signaled that its enforcement priorities will focus on practices that result in patient harm, impact patient care, cause financial loss to federal healthcare programs, are of long duration, or are conducted with actual knowledge the practice is likely to interfere with the access, exchange or use of EHI.

Although the OIG recognizes that it has no authority under the Cures Act to impose information blocking CMPs on providers, providers must comply with separate regulations that relate to data-sharing practices, namely the patient rights of access rules under HIPAA and the CMS attestation requirements. Those programs require eligible clinicians and hospitals to attest that they:

- Did not knowingly and willfully act (such as to disable functionality) to limit or restrict the compatibility or interoperability of certified EHR technology;
- Implemented technologies, standards, policies, practices, and agreements reasonably calculated to ensure, to the greatest extent practicable and permitted by law, that the certified EHR technology was, at all relevant times, connected and compliant with applicable law, accessible to patients, and accessible for trusted exchange with other healthcare providers and certified EHR vendors; and
- Responded in good faith and in a timely manner to requests to retrieve or exchange electronic health information.

For the hospital ADT notifications, look for CMS to issue new or revised survey manual instructions and interpretive guidelines, including how to determine the nature and extent of any deficiencies in assessing noncompliance. Beginning in late 2020, CMS will publicly report clinicians, hospitals, and critical access hospitals (CAHs) that may be information blocking, whether intentional or not. The initial reports will list those clinicians and hospitals participating in the 2019 CMS Promoting Interoperability Program that attested "no" to any of the above attestations as information blockers – on a publicly available CMS website for hospitals and on the Physician Compare website for clinicians. CMS also will publicly report healthcare providers that have digital contact information missing from the National Plan and Provider Enumeration System (NPPES) website. NPPES now maintains a wide range of contact and provider information used to facilitate secure sharing of health information that providers must update within 30 days of any change to avoid the public report of providers with missing information.

Providers may still be subject to CMP liability for knowingly making false statements about the use of certified EHR technology and whether they engage in information blocking through the CMS Promoting Interoperability Programs. Further, a provider that knows a practice is likely to interfere with, prevent, or materially discourage access, exchange or use of EHI would be referred to an appropriate agency for "appropriate disincentives." Further HHS rulemaking will occur to define what these disincentives are, but the OIG states it will refer information blocking claims to the HHS Office for Civil Rights, where a consult on privacy and security rules may resolve the claim.

Bradley's Health Information Technology team is eager to help you understand these rules and how they will impact your contracting and compliance process. Please let us or your regular Bradley attorney know how we can help.

Amy S. Leopard
Partner
aleopard@bradley.com
615.252.2309

Elliot A. Bertasi
Associate
ebertasi@bradley.com
615.252.3530

Jordan Stivers Luke
Associate
jluke@bradley.com
615.252.3542

© 2020 Bradley Arant Boult Cummings LLP

This firm alert is a periodic publication of Bradley Arant Boult Cummings LLP and should not be construed as legal advice or legal opinions on any specific acts or circumstances. The contents are intended only for general information. Consult a lawyer concerning any specific legal questions or situations you may have. No representation is made that the quality of the legal services to be performed is greater than the quality of legal services performed by other lawyers. ATTORNEY ADVERTISING. Rev. 06/2020