33 W Monroe, Suite 1700
Chicago, IL 60603
knicholoff@ehra.org
Phone: 517-930-1198
Twitter: @EHRAssociation

June 23, 2020

Christi A. Grimm
Principal Deputy Inspector General
Office of the Inspector General
Department of Health and Human Services
330 Independence Avenue, SW
Washington, DC 20201

Dear Deputy Inspector Grimm:

On behalf of the 30 members of the Electronic Health Record (EHR) Association, we thank you for the opportunity to share comments on the proposed *Grants, Contracts, and Other Agreements: Fraud and Abuse; Information Blocking; Office of Inspector General's Civil Money Penalty Rules*, which was published in the Federal Register on April 24, 2020.

EHR Association members serve the vast majority of hospitals, post-acute, specialty-specific, and ambulatory healthcare providers using EHRs across the United States. We represent a diverse coalition of stakeholders across the healthcare technology sector, all of whom support the interoperability of health information for patients, healthcare providers, and others working to improve health outcomes. Together, our members represent the world's leading innovators in EHR technology. Our core objective is to collaborate to accelerate health information and technology adoption, advance information exchange between interoperable systems, and improve the quality and efficiency of care through the use of these important technologies.

We appreciate OIG's recognition in its proposed rule that investigating and enforcing information blocking represents a new area of focus. We encourage OIG to take the necessary time to develop expertise in this area and objectively evaluate the impact that information blocking has on HHS programs and their patients. We hope our comments aid OIG in developing this expertise.

Just as OIG is developing foundational knowledge about the health IT industry and information blocking, the member companies of the EHR Association are working to analyze their own responsibilities under the complex new regulatory paradigm created by the Office of the National Coordinator's interoperability rule (ONC Rule). The Association's members also recognize that they are uniquely positioned to support the nation's hospitals, clinics, and other healthcare providers as they work to meet their obligations under the ONC Rule.

Throughout this learning period for the industry, we encourage OIG to build its expertise in this area through collaborative consultation with members of the regulated community, including EHR Association member companies. We would welcome the opportunity to provide additional information to OIG to evaluate and mitigate any adverse impacts that information blocking has on HHS programs and their beneficiaries.

As a first step to this collaboration, we appreciate this opportunity to comment on the Office of the Inspector General's (OIG) proposed enforcement rule and share our recommendations on how ONC and OIG can engage in their information blocking oversight activities in ways that promote interoperability without threatening the innovation and vitality of health IT developers.

Our detailed comments below focus on the following key topics:

- Effective date of OIG's rule and timing considerations for ongoing enforcement;
- Focusing enforcement on activities conducted with actual knowledge;
- Transparency in the complaint and investigation processes;
- Definition of a "violation;" and
- Additional factors OIG should consider when calculating penalty amounts.

The members of the EHR Association remain available to OIG to continue to provide input on reasonable expectations and timelines as we work toward our shared goal of promoting widespread interoperability and protecting patient access to their own health records.

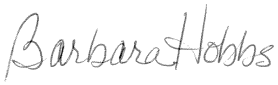
Sincerely,

Cherie Holmes-Henry
Chair, EHR Association
NextGen Healthcare

Hans J. Buitendijk
Vice Chair, EHR Association
Cerner Corporation

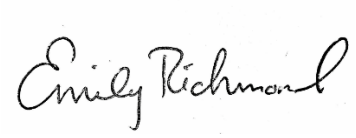
HIMSS EHR Association Executive Committee

David J. Bucciferro
Foothold Technology



Barbara Hobbs
MEDITECH, Inc.

Rick Reeves, RPh
CPSI



Emily Richmond, MPH
Practice Fusion Inc., a subsidiary of Allscripts

Sasha TerMaat
Epic

Courtney E. Tesvich, RN
Nextech

About the HIMSS EHR Association

Established in 2004, the Electronic Health Record (EHR) Association is comprised of more than 30 companies that supply the vast majority of EHRs to physicians' practices and hospitals across the United States. The EHR Association operates on the premise that the rapid, widespread adoption of EHRs will help improve the quality of patient care as well as the productivity and sustainability of the healthcare system as a key enabler of healthcare transformation. The EHR Association and its members are committed to supporting safe healthcare delivery, fostering continued innovation, and operating with high integrity in the market for our users and their patients and families.

The EHR Association is a partner of HIMSS. For more information, visit www.ehra.org.

1. Enforcement Timing

OIG solicited feedback on whether it should make the effective date of its enforcement rule October 1, 2020 rather than the standard period of 60 days following publication of its rule.

We understand that OIG intends for the provisions of its rule "to work in tandem" with the ONC rule; therefore, it would be puzzling for the OIG rule to adopt an effective date that is any sooner than the compliance date established in the ONC Rule: November 2, 2020.[1] In its rule, ONC stated:

> ***OIG and ONC are coordinating timing of the compliance date of the information blocking section of this final rule (45 CFR part 171) and the start of information blocking enforcement****. We are providing the following information on timing for actors. Enforcement of information blocking civil monetary penalties (CMP) in section 3022(b)(2)(A) of the PHSA will not begin until established by future notice and comment rulemaking by OIG. As a result, actors would not be subject to penalties until CMP rules are final.* ***At a minimum, the timeframe for enforcement would not begin sooner than the compliance date of the information blocking section of this final rule (45 CFR part 171)*** *and will depend on when the CMP rules are final. Discretion will be exercised such that conduct that occurs before that time will not be subject to information blocking CMP.*
>
> ***We have finalized § 171.101 with an additional paragraph to codify the compliance date for the information blocking section of this final rule (45 CFR part 171). Section 171.101(b) states that health care providers, health IT developers of certified health IT, health information exchanges, and health information networks must comply with this part on and after November 2, 2020****.*[2]

Therefore, enforcement should not begin on the alternative enforcement date proposed by OIG (October 1, 2020). Instead, we recommend that OIG establish an effective date for its rule that is the later of: (1) six months following publication of the rule in the Federal Register, or (2) February 1, 2021. This approach to OIG's information blocking enforcement effective date would provide regulated entities with much-needed additional time to come into compliance with the many complex provisions of the ONC Rule before being subject to penalties.

Establishing February 1, 2021 as the earliest effective date for the OIG rule also aligns with ONC's announcement of enforcement discretion for its Information Blocking Condition of Certification at 45 CFR 170.401. ONC's announcement indicated to developers of certified health IT that they will not be subject to sanctions under the ONC Health IT Certification program for noncompliance with 45 CFR Part 171 until February 1, 2021. Aligning the effective date of OIG's rule with ONC's enforcement discretion period will help eliminate divergent or confused expectations for health IT developers in the interim, and better coordinates efforts across agencies. Enforcing the ONC Rule's requirements in a thoughtful, consistent, and unified manner, as opposed to a piecemeal approach, would help eliminate uncertainty in the regulated community and reduce the burdens on healthcare stakeholders.

Cooperative Enforcement Period

Once the OIG's rule is effective, we strongly urge OIG to exercise enforcement discretion for the subsequent two years by pursuing cooperative enforcement through the use of corrective action plans. Corrective action plans and resolution agreements could be published while keeping the names of involved parties anonymous as a form of sub-regulatory guidance. This approach would help establish a common understanding for the regulated community of how OIG and ONC interpret the obligations of regulated actors under ONC's Rule.

While members of the EHR Association are committed to preventing information blocking, we recognize OIG may be concerned with bad actors that continue to pursue problematic conduct. During this learning period, if OIG determines that enforcement through civil monetary penalties is necessary, OIG should reserve such fines for entities that are non-cooperative or that act in bad faith. After the two year learning period, OIG could ramp up penalties for all actors to the statutory maximum established in the 21st Century Cures Act.

A rush to penalties may also have a stifling effect on interoperability. Imposing significant fines before stakeholders gain a clear understanding of their obligations, through sub-regulatory guidance and corrective action plans, would deter efforts to innovate and improve the exchange of health information. A period of cooperative enforcement would offer necessary breathing room to promote ongoing collaboration in the industry, while also enabling OIG to address truly problematic practices.

Additionally, COVID-19 has placed unforeseen demands on health IT developers (and our customers) that affect the availability of resources to complete the development and compliance tasks necessary to meet the requirements of ONC's Rule. As healthcare rapidly shifted to virtual care to cope with the impacts of COVID-19, the manner in which electronic health information is created, maintained, exchanged, and used has also rapidly evolved. The broad provisions of the ONC Rule mean these rapidly evolving activities have implications for actors' compliance with ONC's expectations that entities could not have reasonably anticipated.

OIG should acknowledge this reality and the critical role regulated entities have in efforts to combat the pandemic, and provide additional time to evaluate the impact of the ONC Rule and bring activities into compliance. A cooperative enforcement period accomplishes that.

Ongoing Guidance and Education for Regulated Actors

Therefore, during the enforcement discretion period mentioned above or soon after the effective date of OIG's rule, we recommend that OIG devote resources to providing increased clarity to the regulated community on its enforcement priorities, including through an advisory opinion process by which practical guidance could be provided to regulated entities on conduct that would and would not result in the application of information blocking CMPs. OIG could educate regulated entities on the appropriate application of exceptions to information blocking by publishing its advisory opinions (redacting the name of the requesting entity). If an advisory process is too resource intensive for OIG or runs the risk of delaying the timely delivery of actionable insights to regulated entities, we encourage OIG to establish a more lightweight mechanism to receive and respond to questions. This guidance process could take the form of:

- Questions and Answers made available on OIG's website, similar to the informal question and answer portal that OIG has made available for COVID-19 and Anti-Kickback Statute-related questions;

- Frequently Asked Questions documents, similar to those used for many years by ONC to address health IT regulatory clarification (while we recognize that FAQs are not a standard tool used by OIG now, it's a mechanism that the health IT regulatory process is familiar with); or

- Compliance Guidance specifically for health IT developers, health information networks, and health information exchanges similar to the voluntary compliance program guidance documents OIG has developed for hospitals in the fraud, waste, and abuse context.

We note that EHR Association member companies have requested guidance from ONC on areas of its rule that continue to create substantial confusion for the regulated community. The EHR Association has to date submitted nearly 50 questions to ONC, requesting clarification on the requirements embedded in information blocking exceptions that remain a source of uncertainty for the Association's members. These questions address a wide range of requirements and implicated practices under the ONC Rule, and our organizations have yet to see a response from ONC or an indication of when we can expect responses. Our submitted questions include, among others:

- When health IT developers receive an interoperability request that would require additional development work, what is a health IT developer's obligation? Is the non-

existence of an interoperability element an indication that the developer is "technically unable" to meet that content and manner and that it is reasonable to move to an alternative under Content and Manner? Are there other portions of the regulation that would obligate new development?

- Can the actor receiving the request determine that agreeable terms will not be able to be reached and move immediately to an alternative manner under Content and Manner, or must some kind of market-based terms be offered first?

- ONC outlines that the 10-day and 30-day timelines required to meet the licensing exception are triggered by the receipt of a request for license or use of EHI (p. 976), even when the requestor does not understand the need for a license. What needs to occur within the 30-day timeline? Do negotiations need to be completed and a license signed within the 30-day timeframe? A 30-day timeline from the point of request to complete negotiations does not seem realistic for many scenarios. In our experience, many licensing negotiations can take longer than 30 days simply because there are approval processes that must occur on both sides of the negotiation and those approval processes on their own can take quite a bit of time. We ask that ONC allow more time for completion of negotiation as long as it occurs in good faith.

These questions reflect not only lingering ambiguities in the ONC Rule but also the unavoidable mismatch between the complex regulatory framework set out by the ONC Rule and the realities of health IT developers' business practices. Timely responses to these questions are critical to informing EHR Association member companies' compliance activities, and it would be inappropriate for penalty-based enforcement activities to kick off while regulated entities await important clarifying guidance from ONC. We note, too, that even when answers are returned, it will take the industry some time to implement and act on the returned guidance.

2. Enforcement Criteria and Focus

OIG emphasizes in the proposed rule that the definition of information blocking includes an element of "intent" and, as such, the agency "will not bring enforcement action against actors who [OIG] determined made innocent mistakes (i.e., lack the requisite intent for information blocking)."[3] We appreciate and agree with OIG's emphasis on intent because it creates additional clarity for actors who may otherwise be subject to an unfair presumption of information blocking guilt because they "should have known" the potential outcome of a practice. We request that OIG provide additional clarity for regulated actors by expounding on the element of intent to require that actors have direct and clear knowledge that an intentional practice has the effect of impermissible information blocking.

In the proposed rule, OIG identifies the presence of "actual knowledge" as a factor that OIG will consider when prioritizing conduct for enforcement. The requisite element of intent that OIG highlights in its proposed rule is effectively the same as actual knowledge, so we recommend that OIG prioritizes its enforcement based on evidence of actual knowledge. Additionally, it would be helpful if OIG could clarify the relationship between these two terms — "intent" and "actual knowledge" — in its rule. Relying on established tort law, OIG should take the position that an entity acts with the requisite intent to engage in information blocking if: (a) the entity acts with the purpose of information blocking; or (b) the entity acts knowing that information blocking is substantially certain to result.[4] This construct would suggest that in order for impermissible conduct to be carried out with actual knowledge, the conduct must be both voluntary and intended to serve an impermissible purpose (in this case, information blocking).

We appreciate OIG's acknowledgement that "OIG will not bring enforcement actions against actors who OIG determined made innocent mistakes (i.e., lack the requisite intent for information blocking)."[5] We agree that impermissible activities that entities engaged in with actual knowledge must be distinguished from "innocent mistakes," and suggest that OIG expand its interpretation of innocent mistakes to clearly include errors or even negligence that were not intended to result in information blocking. Given the complexity of the ONC Rule's requirements, even the most ethical and conscientious entities might inadvertently make mistakes. Consider the following examples:

- A health IT developer indicates that it is unable to respond to a request to access, exchange, or use electronic health information due to technical limitations, relying on the infeasibility exception; it erroneously does not document its reasoning contemporaneously or in sufficient detail, yet their infeasibility assessment is otherwise sound;

- A client reaches out to an employee who has left the company with a request for connectivity support, thereby not receiving a response. The client files an information blocking complaint rather than addressing with the company;

- An actor updates new contracts for interoperability elements to adhere to the terms of the license agreement, but is unable to unilaterally update historical contracts with its existing customers; or

- A health IT system experiences a downtime that is inadvertent and unplanned, yet the downtime does not fit squarely within the requirements of the performance exception to information blocking.

The EHR Association believes that all of these examples constitute innocent mistakes that lack the requisite intent for information blocking. As OIG evaluates and takes action against entities

that they conclude have the requisite intent, we ask that OIG provide more specific guidance both in its rule and accompanying sub-regulatory guidance on how it will evaluate "intent" in allegations of information blocking.

Please note that as we have stated in other comments to ONC, compliance processes for all relevant parties can be streamlined by defining specific affirmative activities that health IT developers and provider organizations can undertake to prevent information blocking — including supporting standards-based exchange — rather than focusing exclusively on requiring proof that entities are not engaged in information-blocking. We believe this comment is relevant for OIG to consider, as well.

3. Transparency and Coordination with ONC

We encourage OIG to provide greater clarity in its rule regarding how it intends to work with ONC to ensure complaints are valid. ONC's process is not well-defined and could lead to speculative claims. For example, it is unclear how complaints will be filtered by ONC prior to referral to OIG to ensure that concerns and complainants are valid and not arbitrary or capricious. Will there be any process to notify health IT developers of a complaint before it is marked for formal investigation or subpoena? This notification is crucial because where appropriate, regulated entities should have an opportunity to investigate over a reasonable time period, respond to the complaint, and take corrective action before OIG is required to spend resources investigating and pursuing enforcement.

Based on the lack of structure and clarity surrounding the complaint process to date, we are left to assume that it remains a work in progress. It is essential that the complaint process is clearly defined to regulated entities, either in the preamble to OIG's rule or via sub-regulatory guidance, because without the complaint process being clearly defined, enforcement is likely to be spotty and imbalanced, and inherently will mean greater burden on regulated entities as they attempt to prepare for scenarios or investigatory steps that do not materialize.

We note further that the Inspector General's office has a mandate to independently and objectively conduct inspections and evaluations. We are concerned about OIG's ability to maintain the independence necessary for balanced oversight over ONC, given the level of close coordination and deference to ONC that is likely to occur, especially in the initial years of information blocking enforcement.

Similarly, it would also be helpful if OIG could provide additional context on how information blocking investigations will be conducted, perhaps using reference points from OIG's significant experience and expertise investigating activities under other intent-based laws. It would be helpful to understand how OIG's investigatory powers will complement or overlap with ONC's authority to enforce compliance with requirements under the ONC Health IT Certification

Program (which now includes an information blocking compliance attestation). A poorly defined investigatory process makes it hard for entities to plan for the requisite documentation and other supporting resources that might be needed. If regulated entities do not adequately understand what to expect during the investigatory process, it is likely that investigations and any ensuing activities will be costly and burdensome for both regulated entities and OIG.

Additionally, we seek guidance on the data retention period for claims related to information blocking and the retrospective period of review for information blocking claims. Requests for access, use and exchange of EHI are commonplace and are expected to increase following the compliance date of the ONC Rule, and responding to such requests can be a voluminous exercise for health IT developers. Given the lack of clarity as to the scope and breadth of information that should be retained in relation to each EHI request, especially as might be needed to demonstrate the appropriate application of an exception to information blocking, additional guidance from OIG would be helpful, knowing that document collection and retention creates a significant administrative burden.

4. Evaluating Single Versus Multiple Violations

OIG indicates in its Proposed Rule that the "important facts" for determining the number of violations are "the discrete practices that each meet the elements of the information blocking definition." Fundamentally, we suggest that a practice that is representative of an organization's policy should be considered a single practice (based on the organization's single policy), and the number of instances in which that policy has been faithfully implemented could be evaluated as an aggravating factor that impacts the amount of penalties.

Some examples to consider where the situation should be considered a single violation:

- There is an unforeseen hosting outage and multiple clients lose connectivity to their certified products. Would this be classified as a single potential violation or multiple potential violations (one for each affected customer)? While this is not information blocking per se, we are planning to document such events in case an entity or individual were to allege we were withholding information. We must know to what extent we should be creating and retaining documentation.

- A software defect is discovered in the C-CDA document that affects several customers and up to or exceeding thousands of documents a day. Would this be investigated as a single potential violation or multiple potential violations?

- Pricing negotiations are a natural part of our business. When customers purchase multiple offerings, sometimes items are bundled and offered at a discount. What will happen if it is determined that as a result of this common practice, several similarly

situated customers have different pricing? Would that constitute one type of potential violation or multiple potential violations (one for each executed contract)?

In our analysis, the actors in all of these examples would lack intent, and it would be inaccurate to assert the actors were engaged in information blocking. As OIG evaluates and takes action against entities that they conclude have the requisite intent, we ask that OIG provide more specific guidance both in its rule and accompanying sub-regulatory guidance on how it evaluated the intent of sanctioned actors.

5. Factors to Consider in Determining Penalty Amounts

OIG has proposed to codify the statutory factors it must consider when imposing CMPs against an actor for committing information blocking. We agree that these statutory factors are important considerations when evaluating the impact of a particular practice. OIG notes that it has "limited experience to inform the proposal of additional aggravating and mitigating circumstances," and thus solicits comments on "additional factors" it should consider in determining the amount of information blocking CMPs, "including examples of specific conduct that should be subject to higher or lower penalty amounts."[6]

Accordingly, we urge OIG to consider the following mitigating factors when determining the penalty amount for violations, and address in the preamble to its rule how it will evaluate these factors.

Compliance Activities

Regulated entities should get credit for having in place robust compliance programs designed to implement the requirements of the ONC Rule. A compliance program that is tailored to a regulated entity's business and has mechanisms in place to help identify, assess, and mitigate risk (including through suitable training programs, policies, and procedures), should factor into OIG's determination of penalty amounts for any information blocking violations. Similarly, OIG could examine regulated entities' compliance with historical certification expectations under the ONC Health IT Certification Program.

Involvement of Other Entities

When evaluating penalty amounts, OIG should carefully consider the impact of another entity or individual's activities on the impermissible conduct, including the impact of those activities on the outcome or harm resulting from the information blocking conduct. There are myriad public and private sector activities that impact the exchange, access, and use of electronic health information, and we expect that it will take time for OIG to build a foundational understanding of the health IT industry. Health IT developers' role in the access, exchange, and

use of electronic health information is often that of a facilitator. Healthcare providers are the primary data stewards that retain ultimate control and decision-making authority regarding how health information may be disclosed. Consider the following scenarios that illustrate the limited authority of health IT developers:

- What happens when healthcare organization customers decide not to follow a health IT developer's recommended practice for the best use of a software solution? Health IT developers should not be held responsible if their customers deviate from what is standard, or configure software differently than advised.

- Many health IT solutions are specifically architected to be flexible. If a healthcare organization pays its health IT developer to configure a health IT solution in a non-standard way (against the health IT developer's recommendations), the health IT developer should not be at risk of being held responsible for issues that arise related to information blocking.

Flexibility and Evolution of Health IT

EHR Association member companies give healthcare providers a broad choice of tools, functionality, and other services they can use to access, exchange, and use electronic health information. In the vast majority of cases, it is up to healthcare provider organizations which tools they use to fulfill a request to access, exchange, or use electronic health information. OIG should take into account the flexibility of health IT solutions and the alternative options that may have been available to support a particular access, exchange, or use of electronic health information.

Self-Disclosure and Voluntary Correction

Under the proposed rule, OIG indicates that information blocking would be subject to OIG's standard CMP procedures and appeals process (see 42 CFR Parts 1003 and 1005). OIG is soliciting comments on the proposed incorporation of the information blocking regulations into 42 CFR part 1003, and the proposed application of the existing CMP procedures and appeal process in parts 1003 and 1005 to the information blocking CMP. We would like to offer another avenue for consideration, in addition to or in lieu of an appeals process: a self-disclosure process.

The EHR Association believes that designing and implementing a self-disclosure protocol, in conjunction with ONC, would create a culture of transparency, trust, and compliance between the disclosing parties and the oversight bodies, and will promote long-term compliance with ONC health IT regulation.

As health IT developers and providers work to implement the requirements of ONC's 21st Century Cures Act Rule, there will be circumstances when they encounter an issue that will require resolution. For example, developers must create a Real World Testing Plan by December 15, 2020 with eventual results to be published publicly on the Certified Health Product List (CHPL). During the creation and development of these plans, there will potentially be areas where developers will encounter errors and defects that they must work through as part of that new process.

OIG has experience in implementing this type of program, for example through its Provider Self-Disclosure Protocol. We encourage OIG to develop a similar program for information blocking enforcement. Typically, self-disclosure leads to lesser penalties and a smoother process with OIG in terms of disclosure, corrective action, and penalties.

---

[1] 85 Federal Register
[2] 85 Fed. Reg. 25642, 25792-93 (May 1, 2020) (Emphasis added)
[3] 85 Federal Register 22984
[4] Restatement (Third) of Torts: Liab.for Physical & Emotional Harm § 1(b)
[5] 85 Federal Register 22984
[6] 85 Federal Register 22987