June 22, 2020

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

Submitted electronically at: https://www.federalregister.gov/documents/2020/04/24/2020-08451/grants-contracts-and-other-agreements-fraud-and-abuse-information-blocking-office-of-inspector

RE: Grants, Contracts, and Other Agreements: Fraud and Abuse; Information Blocking; Office of Inspector General's Civil Money Penalty Rules

Ms. Grimm:

AMIA appreciates the opportunity to comment on OIG's proposed approach to establishing civil monetary penalties (CMPs) for information blocking.

AMIA is the professional home for more than 5,500 informatics professionals, representing frontline clinicians, researchers, public health experts, and educators who bring meaning to data, manage information, and generate new knowledge across the research and healthcare enterprise. As the voice of the nation's biomedical and health informatics professionals, AMIA plays a leading role in advancing health and wellness by moving basic research findings from bench to bedside, and evaluating interventions, innovations and public policy across care settings and patient populations.

Before addressing the specifics of OIG's proposals, we wish to reiterate two key concepts conveyed to the Office of the National Coordinator for Health IT during its development of policies at 45 CFR 170 and 171.

First, we note that "information blocking" is not simply the absence of interoperability. As depicted in our "Socio-Technical Interoperability Stack," (see Appendix A) interoperability may not occur for myriad reasons. In addition to being dependent on standards for syntax, semantics, and transport, interoperability within the healthcare context needs agreement on when and how data should be presented within workflows. Which data appear in a patient's record on what timeline may change depending on clinical workflows, types of data, and patient characteristics. Healthcare

interoperability also depends on a host of public policies, such as 42 CFR Part 2 or HIPAA, as well as business drivers, intellectual property, contractual obligations, and medico-legal interpretations.

As OIG investigate claims of information blocking, **AMIA recommends using this Socio-Technical Interoperability Stack to inform its decisions to pursue CMPs and enhance its understanding of the healthcare interoperability ecosystem.** For example, impeded information flows stemming from the "traditional technology stack" (depicted in red) may warrant closer scrutiny than information impediments occurring higher above the stack because the traditional technology stack of standards will likely be more fully in the control of health IT developers, HIEs and HINs. We also note that some of the factors depicted in the socio-technical stack may be covered by one or another of the Exceptions established by ONC (e.g. HIPAA's minimum necessary inhibiting sharing of an irrelevant test result).

Second, we recommend that OIG foster a period of learning during its proposed enforcement discretion and in the subsequent, initial months of the program. Understanding the particulars of information blocking claims and exceptions will be important for all stakeholders so that clarifying guidance and educational information can be broadly disseminated. To this end, **AMIA recommends that OIG establish an effective date 60 days following publication of a final rule in the *Federal Register*, followed by a period of enforcement discretion between three and six months.** This additional time will help actors establish necessary policies and protocols to comply with newly effective ONC rules and give OIG additional time to receive feedback from health IT developers, health information exchanges and health information networks (HIEs/HINs).

Additionally, **AMIA recommends that information blocking claims and scenarios where actors are relying on information blocking exceptions are (1) well-documented; (2) reviewed in a timely manner; and (3) publicly available online in a searchable manner.** If claims do not lead to enforcement cases, or if the exception is valid, AMIA recommends OIG blind or anonymize the actors involved, focusing on the facts of the case. The underlying aim should be to create the enforcement conditions that compel proper actions, deter improper actions, and create an educational environment for all actors to understand what differentiates the two. This would be consistent with other lines of investigation conducted by OIG[1] and would help foster a cycle of continuous improvement.

Finally, we understand that this Proposed Rule on Information Blocking Enforcement does not apply to health care providers. Given there is a subsequent proposed rule specifically addressing information blocking enforcement for health care providers, we recommend OIG include preamble discussion of the process for enforcement, priorities, timeline, expected agencies to refer health care providers to, and appropriate disincentives to be applied to providers. Such information will help providers understand their role and help them better comply.

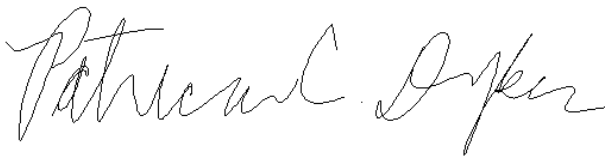
[1] Civil Monetary Penalties and Affirmative Exclusions. Available at: https://oig.hhs.gov/fraud/enforcement/cmp/index.asp

AMIA | American Medical Informatics Association
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

June 22, 2020

We hope our comments are helpful as you undertake this important work. Should you have questions about these comments or require additional information, please contact Jeffery Smith, Vice President of Public Policy at jsmith@amia.org or (301) 657-1291. We look forward to continued partnership and dialogue.

Sincerely,



Patricia C. Dykes, PhD, RN, FAAN, FACMI
Chair, AMIA Board of Directors
Program Director Research
Center for Patient Safety, Research, and Practice
Brigham and Women's Hospital

(Enclosure: AMIA Recommendations to OIG Re: Information Blocking Civil Money Penalty Rules)

June 22, 2020

SUBPART N—CMPS FOR INFORMATION BLOCKING

OIG has authority to investigate and discretion to choose which information blocking complaints to investigate. OIG focuses on selecting cases for investigation that are consistent with enforcement priorities, which based on current expectations, include conduct that:

(i) Resulted in, is causing, or had the potential to cause patient harm;
(ii) Significantly impacted a provider's ability to care for patients;
(iii) Was of long duration;
(iv) Caused financial loss to Federal health care programs, or other government or private entities; or
(v) Was performed with actual knowledge.

- OIG lacks the authority to pursue information blocking CMPs against actors who OIG concludes did not have the requisite intent. Consequently, OIG will not bring enforcement actions against actors who OIG determined made innocent mistakes (i.e., lack the requisite intent for information blocking).
- OIG may refer an information blocking claim to OCR if a consultation regarding the health privacy and security rules promulgated under sec. 264(c) of HIPAA would resolve an information blocking claim.
- OIG will not begin enforcing the information blocking CMPs until the OIG CMP information blocking regulations are effective.

AMIA Recommendations: AMIA supports this approach and understands OIG's limitations. However, we recommend that OIG remove (v) from listed types of enforcement priorities because it is duplicative. If a precondition for enforcement is intent, the priority of "was performed with actual knowledge," is unnecessary. Instead, we encourage OIG to prioritize conduct that "hinders HHS goals or violates multiple programmatic policies." For instance, ONC has recently established new Conditions and Maintenance of Certification requirements for health IT developers and is implementing the trusted exchange framework and common agreement (TEFCA). Actions that violate a Condition of Certification or inhibit the functioning of TEFCA should be monitored – and if uncovered – penalized. Falsely attesting to the absence of data blocking in MIPS or other quality/payment programs reporting would be another example.

Effective Date & Enforcement

OIG proposes that the effective date of these regulations be 60 days from the date of publication of the final rule. OIG is also considering an alternative proposal that would establish a specific date that OIG's information blocking CMP regulations would be effective. Specifically, OIG is considering for the final rule an effective date of October 1, 2020 for subpart N of part 1003. OIG solicits comment on these proposed approaches for the effective date of OIG's information

blocking CMP regulations, which would subsequently determine the start of OIG's information blocking enforcement.

AMIA Recommendation: We note that according to 5 U.S.C. § 801(a)(3)(A), major rules must be published in the *Federal Register* at least 60 days prior to their effective date.[2] While we support enforcement discretion, we ask OIG to clarify that such time period begin following an effective date established 60 days after publication in the *Federal Register*. Furthermore, we reiterate our recommendation that this enforcement discretion period extend three to six months after the final rule's effective date.

§ 1003.1400—BASIS FOR CIVIL MONEY PENALTIES

Pursuant to sec. 3022(b)(2)(B), the CMP authority does not extend to health care providers. If OIG determines that a health care provider has committed information blocking, it shall refer such health care provider to the appropriate agency for appropriate disincentives. The appropriate agency and appropriate disincentives will be established by the Secretary in future notice and comment rulemaking. OIG will coordinate closely with other agencies within HHS to develop consultation and referral processes consistent with such rulemaking by the Secretary.

AMIA Recommendation: Generally, we support this approach articulated by OIG and efforts to establish HHS-wide procedures for health care providers found to be information blocking. In anticipation of a subsequent rulemaking for these actors, we recommend OIG consider including a Corrective Action Plan (CAP) as part of the process of investigating, evaluating, finalizing, and consider CMPs against actors. This is a common practice done by several other agencies within HHS, including OCR's enforcement of the HIPAA Privacy and Security rules. We believe that the opportunity to have a CAP incorporated into the enforcement process will more actively promote the needed lasting change in a possible information blocking practice, with less financial and litigation burden.

§ 1003.1410

OIG propose to add a new § 1003.1410 to codify the maximum penalty OIG can impose per violation of the PHSA's information blocking provisions. PHSA sec. 3022(b)(2)(A) authorizes a maximum penalty not to exceed $1,000,000 per violation. Furthermore, OIG proposes to define "violation" as each practice that constitutes information blocking. OIG solicits comment on the proposed definition of "violation," and examples of what constitutes a single violation.

[2] 5 USC 801. Available at: https://www.law.cornell.edu/uscode/text/5/801

AMIA Recommendation: We agree with and support OIG's proposal to define "violation" as each practice that constitutes information blocking. However, we encourage OIG to view a repetitive practice, like the example illustrated at 85 FR 22987, [3] as an aggravating factor, rather than a multiplying factor. Further, we encourage OIG to establish ongoing examples based on real cases to help stakeholders learn and comply with information blocking prohibitions.

§ 1003.1420

OIG proposes to add a new § 1003.1420 that would codify the factors that are considered when imposing a CMP against an individual or entity for committing information blocking. PHSA sec. 3022(b)(2)(A) mandates that a determination to impose a CMP for an information blocking violation must consider factors such as

- The nature and extent of the information blocking
- The harm resulting from such information blocking, including, where applicable,
    - The number of patients affected,
    - The number of providers affected, and
    - The number of days the information blocking persisted.

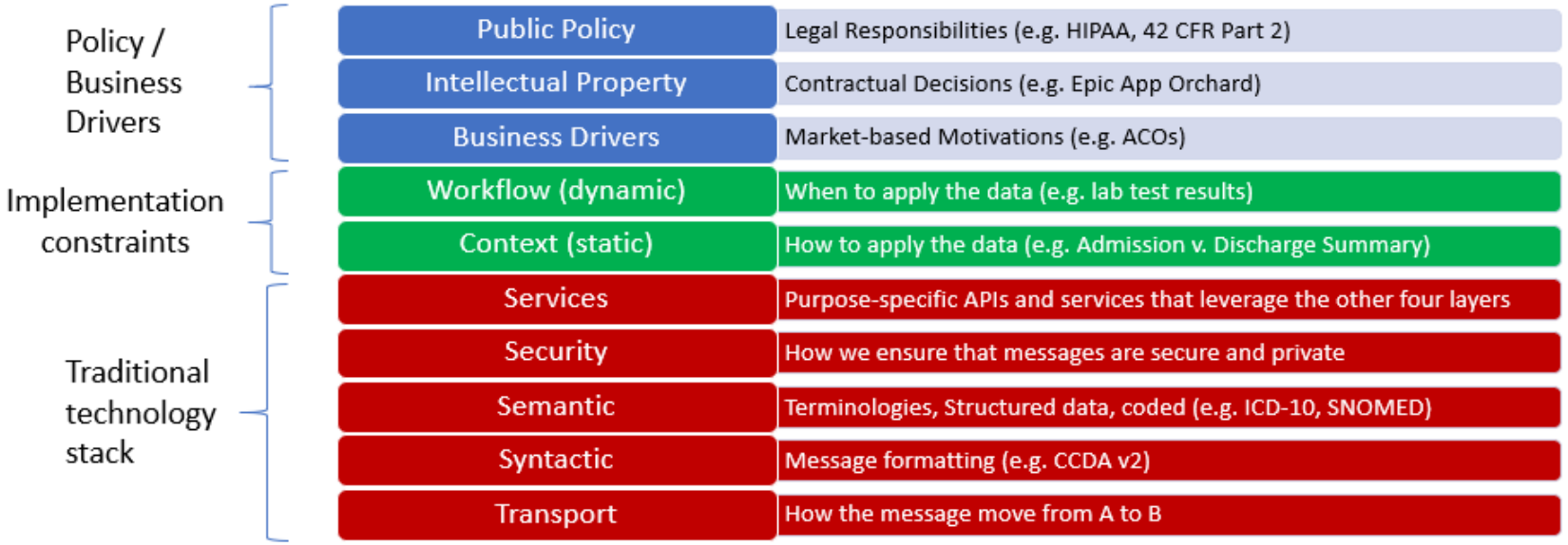
We solicit comments on any additional factors we should consider, for purposes of a final rule, in determining the amount of information blocking CMPs, including examples of specific conduct that should be subject to higher or lower penalty amounts.

AMIA Recommendations: We believe these priorities are the right ones for health IT developers and HINs/HIEs. An additional priority over the near-term is the degree to which information blocking affects public health/community health – particularly as we continue to face health IT challenges addressing the current COVID-19 Pandemic. Additionally, we recommend OIG consider the history of compliance with the provisions (first-time offenders vs. repeat offenders) and the commercial status of the actor (nonprofit entities vs. for-profit entities) when considering CMPs.

[3] 85 FR 22987. Available at: https://www.federalregister.gov/d/2020-08451/p-100

Appendix A: Sociotechnical Interoperability Stack

Information Blocking and the Socio-Technical Stack



AMIA | American Medical Informatics Association
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814