REPORT TO CONGRESS

APRIL 2015

Report on Health Information Blocking

Prepared by:

The Office of the National Coordinator for Health Information Technology (ONC)

Department of Health and Human Services

200 Independence Avenue SW

Washington, DC 20201

Submitted to:

The Honorable Tom Cole, Chairman, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations

The Honorable Rosa DeLauro, Ranking Member, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations

The Honorable Roy Blunt, Chairman, Subcommittee on Labor, Health and Human Services, Education, and Related Agencies, Committee on Appropriations

The Honorable Patty Murray, Ranking Member, Subcommittee on Labor, Health and Human Services, Education, and Related Agencies, Committee on Appropriations

TABLE OF CONTENTS

EXECUTIVE SUMMARY **4**

PURPOSE OF REPORT **5**

CONGRESSIONAL REQUEST **5**

ONC'S RESPONSIBILITY TO ANSWER REQUEST **5**

I. INTRODUCTION **6**

Information Blocking and its Potential Impacts 7

Overview of Findings and Recommendations in this Report 8

II. WHAT IS INFORMATION BLOCKING? **11**

Definition and Criteria 11

Distinguishing Information Blocking from Other Barriers to Interoperability and Health Information Exchange 12

Conduct That Raises Information Blocking Concerns 12

Countervailing Interests 13

III. DESCRIPTION OF KNOWN EXTENT OF INFORMATION BLOCKING **15**

Anecdotal Evidence of Potential Information Blocking 15

Empirical Data and Research on Health Information Exchange 18

Where Knowledge of Information Blocking is Limited and How to Resolve 19

IV. CHARACTERISTICS OF A COMPREHENSIVE STRATEGY TO LIMIT INFORMATION BLOCKING **21**

Need for a Comprehensive Approach 21

Targeted Actions to Address Information Blocking 21

Gaps and Additional Areas for Consideration 29

CONCLUSION **33**

APPENDIX A — INFORMATION BLOCKING SCENARIOS **34**

APPENDIX B — ONC HIT CERTIFICATION PROGRAM **39**

EXECUTIVE SUMMARY

This report responds to Congress's request for the Office of the National Coordinator for Health Information Technology (ONC) to produce a report on the extent of health information blocking and a comprehensive strategy to address it.

An examination of these issues is both timely and warranted. Since the enactment of the HITECH Act and subsequent legislation, the federal government has invested over $28 billion to accelerate the development and adoption of health information technology (health IT). The purpose of these efforts is to enable an interoperable learning health system—one in which electronic health information is available and can be securely and efficiently shared, when and where it is needed, to support patient-centered care, enhance health care quality and efficiency, and advance research and public health.

While many stakeholders are committed to achieving this vision, current economic and market conditions create business incentives for some persons and entities to exercise control over electronic health information in ways that unreasonably limit its availability and use. Indeed, complaints and other evidence described in this report suggest that some persons and entities are interfering with the exchange or use of electronic health information in ways that frustrate the goals of the HITECH Act and undermine broader health care reforms. These concerns likely will become more pronounced as both expectations and the technological capabilities for electronic health information exchange continue to evolve and mature.

As more fully defined in this report, information blocking occurs when persons or entities knowingly and unreasonably interfere with the exchange or use of electronic health information. This report provides principled and practical criteria for identifying such conduct and distinguishing it from other barriers to interoperability and health information exchange. It also examines the nature and extent of information blocking, based on available evidence and the accumulated industry knowledge and experience of ONC. While the evidence is in some respects limited, there is little doubt that information blocking is occurring and that it is interfering with the exchange of electronic health information.

ONC believes that information blocking is best addressed through a combination of targeted actions aimed at deterring and remedying information blocking, and broader strategies and approaches that engage the larger context in which information blocking occurs. This report details actions that ONC is currently taking or has proposed to take, in coordination with the Department of Health and Human Services (HHS) and other federal agencies, to target and address information blocking.

While important, these actions alone will not provide a complete solution to the information blocking problem. Indeed, a key finding of this report is that many types of information blocking are beyond the reach of current federal law and programs to address. Thus a comprehensive approach will require overcoming significant gaps in current knowledge, programs, and authorities that limit the ability of ONC and other federal agencies to effectively target, deter, and remedy this conduct, even though it frustrates the important public policy of enabling electronic health information to flow in support of patients and improvements in health and health care.

For these reasons, in addition to the actions outlined in this report, successful strategies to prevent information blocking will likely require congressional intervention. ONC believes there are several avenues open to Congress to address information blocking, including the gaps identified in this report, to ensure continued progress towards the nation's health IT and health care goals. We are continuing to analyze those gaps and look forward to working with Congress to identify the best solutions.

PURPOSE OF REPORT

CONGRESSIONAL REQUEST

The Consolidated and Further Continuing Appropriations Act, 2015[1] was signed by the President on December 16, 2014. An explanatory statement[2] accompanying the Act and agreed to by the House of Representatives and the Senate provides in pertinent part:

> *Information Blocking.--The Office of the National Coordinator for Health Information Technology (ONC) is urged to use its certification program judiciously in order to ensure certified electronic health record technology (CEHRT) provides value to eligible hospitals, eligible providers and taxpayers. ONC should use its authority to certify only those products that clearly meet current meaningful use program standards and that do not block health information exchange. ONC should take steps to decertify products that proactively block the sharing of information because those practices frustrate congressional intent, devalue taxpayer investments in CEHRT, and make CEHRT less valuable and more burdensome for eligible hospitals and eligible providers to use. The agreement requests a detailed report from ONC no later than 90 days after enactment of this act regarding the extent of the information blocking problem, including an estimate of the number of vendors or eligible hospitals or providers who block information. This detailed report should also include a comprehensive strategy on how to address the information blocking issue.*

The explanatory statement also provides:

> *Interoperability.--The agreement directs the Health IT Policy Committee to submit a report to the House and Senate Committees on Appropriations and the appropriate authorizing committees no later than 12 months after enactment of this act regarding the challenges and barriers to interoperability. The report should cover the technical, operational and financial barriers to interoperability, the role of certification in advancing or hindering interoperability across various providers, as well as any other barriers identified by the Policy Committee.*

ONC'S RESPONSIBILITY TO ANSWER REQUEST

This report responds to Congress's request for ONC to produce a report, within 90 days of enactment, regarding the extent of the information blocking problem and a comprehensive strategy to address it. ONC plans to work with the HIT Policy Committee (HITPC) to address Congress's separate request for a report on barriers to interoperability within 12 months.

---

[1] Pub. L. 113-235.

[2] 160 Cong. Rec. H9047, H9839 (daily ed. Dec. 11, 2014) (explanatory statement submitted by Rep. Rogers, chairman of the House Committee on Appropriations, regarding the Consolidated and Further Continuing Appropriations Act, 2015).

I. INTRODUCTION

The secure, efficient, and effective sharing and use of electronic health information when and where it is needed is a key component of health care delivery system reform. The widespread adoption and use of interoperable health information technology (health IT) will enable individuals, providers, and entities to capture, exchange, and use valuable health information to improve decision-making; deliver more effective, patient-centered care; and implement systems and processes to measure and improve health care quality and efficiency. These information and tools also support new models and approaches to health care delivery and payment, create new opportunities for biomedical and other research, and enable major improvements in public health.

Recognizing the importance of health IT and health information exchange for transforming health and health care, and to advance this important public policy, Congress passed the Health Information Technology for Economic and Clinical Health (HITECH) Act in 2009.[3] The HITECH Act charged ONC with coordinating federal policies and investments to support the development of a nationwide health IT infrastructure that would enable and support the kinds of robust health information exchange that Congress envisioned. The HITECH Act also stimulated demand for the adoption and use of health IT by authorizing the Medicare and Medicaid EHR Incentive Programs. To date, these programs have provided more than $28 billion[4] in incentive payments to health care professionals and hospitals that have attested to adopting and meaningfully using electronic health records (EHRs) certified by ONC.

The Patient Protection and Affordable Care Act[5] (ACA), enacted in 2010, further emphasizes the role of health IT and health information exchange in transforming health and health care. The ACA provides incentives for the use of health IT and health information exchange, both through direct requirements for the use of health IT in certain quality reporting programs, and indirectly through new reimbursement policies and value-based payment programs that require advanced health IT and health information exchange capabilities.[6]

Together, these efforts have dramatically increased adoption of EHRs throughout the nation and stimulated demand for a growing range of health IT and health information exchange products, services, and capabilities. Prior to the HITECH Act, health IT adoption among providers and hospitals was just beginning and moving slowly. Today, over three-quarters of eligible providers and nine-in-ten eligible hospitals have received incentive payments for adopting and meaningfully using certified health IT, and more than six in ten hospitals have electronically exchanged patients' health information with providers

---

[3] Pub. L. 111-5, Division A, Title XIII, & Division B, Title IV.

[4] CMS, *Monthly Payment and Registration Summary Report* (Dec. 2014). http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/December2014_SummaryReport.pdf. In addition to payments under the EHR Incentive Programs, Congress directed ONC to invest $2 billion in immediate funding to strengthen the nation's health IT infrastructure, including through investments in health IT implementation assistance, state grants to support health information exchange, and health IT demonstration, education, and workforce programs.

[5] Patient Protection and Affordable Care Act, Pub. L. 111-148.

[6] HHS recently announced an aggressive timeline for shifting Medicare reimbursement from volume to value. HHS, *Better, Smarter, Healthier: In Historic Announcement, HHS Sets Clear Goals and Timeline for Shifting Medicare Reimbursements from Volume to Value*, http://www.hhs.gov/news/press/2015pres/01/20150126a.html (Jan 26, 2015). Private payers have also signaled an increasing commitment to moving to value-based purchasing models. Reed Abelson, *Industry Group to Back Results-Focused Care*, NYTIMES.COM (Jan 28, 2015), available at http://www.nytimes.com/2015/01/28/business/28payment html?_r=2.

outside their organization, a 51 percent increase since 2008.[7] Physicians who have adopted and meaningfully used certified health IT have reported significantly higher clinical, workflow, and financial benefits than those who either don't have an EHR or have an EHR that does not meet the criteria for meaningful use.[8] In addition, a majority of research studies have cited positive health care quality, safety, and efficiency from the effects of certified health IT functionalities.[9]

Yet despite this progress, and for reasons that are both varied and complex, significant challenges continue to limit the widespread and effective sharing of electronic health information across the health care continuum. Many of these challenges are well understood and are being addressed through a diverse range of public and private sector activities. These efforts and additional actions needed to achieve the nation's health IT goals are described in detail in the *Federal Health IT Strategic Plan, 2015–2020*[10] and ONC's draft *Shared Nationwide Interoperability Roadmap*, released for public comment on Jan 30, 2015.[11]

Information Blocking and its Potential Impacts

In contrast to these well-known interoperability challenges, the extent to which information blocking is impeding the effective sharing of electronic health information is less clear. While ONC and others are studying the problem, formal research is limited and anecdotal evidence is often difficult to interpret and still more difficult to generalize.

The term "information blocking" presents significant definitional challenges. There are many types of electronic health information and just as many factors that can inhibit its effective exchange and use. Many actions that prevent information from being exchanged may be inadvertent, resulting primarily from economic, technological, and practical challenges that have long prevented widespread and effective information sharing.[12] Further, even conscious decisions that prevent information exchange may be motivated by and advance important interests, such as protecting patient safety, that further the potential to improve health and health care. These interests must be carefully balanced with the potential benefits from sharing of electronic health information. Finally, it is important to acknowledge that certain constraints on the exchange of electronic health information are appropriate and necessary to comply with state and federal privacy laws; this is not considered information blocking.

---

[7] ONC, *October 2014 Report to Congress: Update on the Adoption of Health Information Technology and Related Efforts to Facilitate the Electronic Use and Exchange of Health Information*, http://www.healthit.gov/sites/default/files/rtc_adoption_and_exchange9302014.pdf.

[8] ONC, *Percent of Physicians with EHRs Agreeing their EHR has the Following Impacts*, Health IT Quick-Stat #8 (2013), http://dashboard healthit.gov/quickstats/pages/EHR-Impacts.php.

[9] ONC, *Effects of Meaningful Use Functionalities on Health Care Quality, Safety and Efficiency, By Study Outcome Result (% of Studies)*, Health IT Quick-Stat #13 (2014), http://dashboard.healthit.gov/quickstats/pages/FIG-Health-IT-Literature-Review-Summary-of-Author-Sentiments.php.

[10] ONC, *Federal Health IT Strategic Plan 2015-2020* (2014) (Draft), available at http://www.healthit.gov/sites/default/files/federal-healthIT-strategic-plan-2014.pdf.

[11] ONC, *Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap Draft Version 1.0* (2015) (hereinafter "Roadmap"), available at http://www healthit.gov/sites/default/files/nationwide-interoperability-roadmap-draft-version-1.0.pdf.

[12] *See generally*, Niam Yaraghi, *A Sustainable Business Model for Health Information Exchange Platforms: The Solution to Interoperability in Healthcare IT* (2015), http://www.brookings.edu/research/papers/2015/01/30-sustainable-business-model-health-information-exchange-yaraghi.

Despite these complexities, ONC believes that there are important reasons to examine information blocking. Allegations continue to surface that some health care providers and health IT developers are interfering with the exchange or use of electronic health information in ways that frustrate the goals of the HITECH Act and undermine broader health care reforms.[13] In addition, current economic incentives and characteristics of both health care and health IT markets create business incentives for some market participants to pursue and exercise control over information in ways that significantly limit its availability and use.[14] And as health information exchange becomes more technologically and financially feasible for many stakeholders, some persons and entities will inevitably regard this trend towards greater information sharing and data liquidity as contrary to their specific business or economic interests. These actors may resist or even seek to prevent the sharing of health information.

Meanwhile, information blocking not only interferes with effective health information exchange but also negatively impacts many important aspects of health and health care. To make informed health care decisions, providers and individuals must have timely access to information in a form that is usable. When health information is unavailable, decisions can be impaired—and so too the safety, quality, and effectiveness of care provided to patients. Information blocking also impedes progress towards reforming health care delivery and payment because sharing information seamlessly across the care continuum is fundamental to moving to a person-centered, high-performing health care system. Further, information blocking can undermine consumers' confidence in their health care providers by preventing individuals from accessing their health information and using it to make informed decisions about their health and health care. And information blocking also prevents advances in biomedical and public health research, which require the ability to analyze information from many sources in order to identify public health risks, develop new treatments and cures, and enable precision medicine.

For all of these reasons, a closer examination of the nature, extent, and potential causes of information blocking is timely and warranted.

Overview of Findings and Recommendations in this Report

Information blocking occurs when persons or entities knowingly and unreasonably interfere with the exchange or use of electronic health information. This report focuses on potential information blocking by health care providers and health IT developers, including vendors of EHR technology.[15]

---

[13] Allegations and other evidence of information blocking are described at length in section III of this report.

[14] *See, e.g.,* Yaraghi, supra n. 12, at 7 (expecting that in the near term, "dominant EHR vendors will have an even greater incentive to only enable the capability of exchanging information between their own products"); Thomas C. Tsai & Ashish K. Jha, *Hospital Consolidation, Competition, and Quality: Is Bigger Necessarily Better?*, 312 J. AM. MED. ASSOC. 29, 29 (2014) (explaining that some large health systems may lack incentives to exchange electronic health information because such "information is seen as a tool to retain patients within their system, not as a tool to improve care."); Dan Gilman & James Cooper, *There is a Time to Keep Silent and a Time to Speak, the Hard Part is Knowing Which is Which: Striking the Balance Between Privacy Protection and the Flow of Health Care Information*, 16 MICH. TELECOMM. TECH. L. R. 279, 298 (2010) ("[S]ome providers may worry that interoperable HIT can facilitate 'business going out the door;' . . . . Lowering the costs of the flow of information may be generally beneficial for consumers and competition, but it is not necessarily beneficial for all competitors.").

[15] This focus is appropriate because providers and developers are the primary financial beneficiaries of the EHR Incentive Programs and, at this stage in the development of the nation's health IT infrastructure, exercise the greatest influence and control over how electronic health information is captured, exchanged, and used throughout the health care system. In addition, most complaints and allegations of information blocking, including those reported to ONC,

The following sections of this report examine the nature and extent of information blocking and identify the elements of a comprehensive approach to address it.

Section II establishes a principled definition of information blocking and explains the many practical and policy considerations that inform that definition. It also provides criteria for identifying and distinguishing information blocking from other barriers to interoperability and health information exchange; identifies certain general categories of business practices and other conduct that raise serious information blocking concerns; and explains the need to carefully analyze competing interests and unique circumstances in individual cases.

Section III examines the nature and known extent of information blocking, based on available evidence, including complaints, other anecdotal evidence, economic and empirical research, and the accumulated knowledge and experience of ONC staff. This section also identifies areas in which evidence of information blocking is limited, and suggests ways to improve evidence and knowledge of information blocking.

Section IV builds on the insights developed in earlier sections and lays out the elements of a comprehensive approach for addressing the information blocking problem. These elements are previewed in Table 1 on the following page and include both targeted actions to mitigate information blocking as well as broader strategies that address the underlying causes of this conduct. In addition, a comprehensive approach will require overcoming significant gaps in current knowledge, programs, and authorities that limit the ability of the federal government and private sector to effectively address information blocking. ONC believes there are several avenues open to Congress to resolve these gaps, which are described at the end of this report.

---

concern the actions of providers and developers. Nevertheless, other persons and entities also hold or facilitate the exchange of electronic health information and may engage in information blocking. Though beyond the scope of this report, an analysis of information blocking by these additional persons and entities is necessary to a complete understanding of the problem.

TABLE 1 — ELEMENTS OF A COMPREHENSIVE INFORMATION BLOCKING APPROACH

Targeted Actions	Broader Strategies
• Strengthen in-the-field surveillance of health IT certified by ONC. • Constrain standards and implementation specifications for certified health IT. • Promote greater transparency in certified health IT products and services. • Establish governance rules that deter information blocking. • Work in concert with the HHS Office for Civil Rights to improve stakeholder understanding of the HIPAA Standards related to information sharing. • Coordinate with the HHS Office of Inspector General and the Centers for Medicare and Medicaid Services concerning information blocking in the context of the federal Anti-Kickback Statute and Physician Self-referral Law. • Refer illegal business practices to appropriate law enforcement agencies. • Work with CMS to coordinate health care payment incentives and leverage other market drivers to reward interoperability and exchange and discourage information blocking. • Promote competition and innovation in health IT and health care.	• Continue public and private sector collaboration to develop and drive the consistent use of standards and standards-based technologies that enable interoperability. • Establish effective rules and mechanisms of engagement and governance for electronic health information exchange. • Foster a business, clinical, cultural, and regulatory environment that is conducive to the exchange of electronic health information for improved health care quality and efficiency. • Clarify requirements and expectations for secure and trusted exchange of electronic health information, consistent with privacy protections and individuals' preferences, across states, networks, and entities.
Address Gaps in Current Knowledge, Programs, and Authorities	
• Limited evidence and knowledge of information blocking. • Limitations of certification for addressing information blocking by developers. • Limitations of program oversight for addressing information blocking by providers. • Inadequate legal protections and enforcement mechanisms for information blocking. • Lack of transparency and information about health IT products and services. • Need for an effective governance mechanism for nationwide health information interoperability.	

II. WHAT IS INFORMATION BLOCKING?

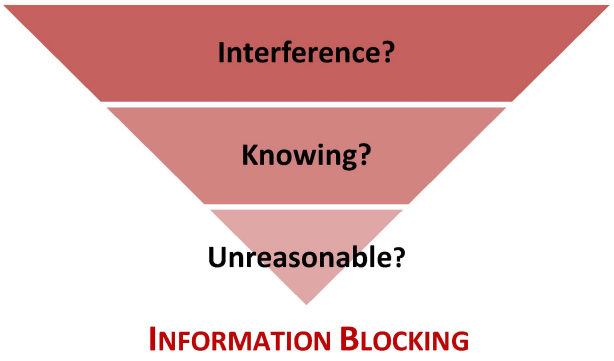
Information blocking means different things to different people and entities. No authoritative or commonly accepted definition exists. To gain a better understanding of the nature and extent of information blocking, ONC collected and reviewed complaints, anecdotes, and available evidence and research; invited stakeholders to share additional anecdotes and perspectives; and considered the opinions of industry observers who have publicly analyzed and commented on information blocking.[16]

The goal of this systematic approach was to establish a practical definition and set of criteria for identifying information blocking and distinguishing it from other kinds of conduct that interfere with health information exchange. This definition and criteria are stated below, followed by an explanation of the practical and policy considerations on which they are based. In addition, Appendix A contains a number of hypothetical scenarios, based on complaints and anecdotes reported to ONC, that illustrate how these criteria can be applied to a variety of real-world situations and actors who may engage in information blocking.

Definition and Criteria

Information blocking occurs when persons or entities knowingly and unreasonably interfere with the exchange or use of electronic health information.

This definition requires three criteria be met:



1. **Interference.** Information blocking requires some act or course of conduct that interferes with the ability of authorized persons or entities to access, exchange, or use electronic health information. This interference can take many forms, from express policies that prohibit sharing information to more subtle business, technical, or organizational practices that make doing so more costly or difficult.

2. **Knowledge.** The decision to engage in information blocking must be made knowingly. An individual or entity does not engage in information blocking unless it knows (or should know under the circumstances) that its conduct is likely to interfere with the exchange or use of electronic health information.

3. **No Reasonable Justification.** Not all conduct that knowingly interferes with electronic health information exchange is information blocking. Accusations of information blocking are serious and should be reserved for conduct that is objectively unreasonable in light of public policy.[17] Public policy must be balanced to advance important interests, including furthering the availability of electronic health information as needed for authorized and important purposes; protecting and

[16] Further discussion of evidence and methods is contained in section III of this report.
[17] Conduct that is required to comply with federal or state privacy law would not be "unreasonable" and would not constitute information blocking under these criteria.

promoting patient safety; maintaining the privacy and security of electronic health information; and protecting the legitimate economic interests and incentives of providers, developers, and other market participants to innovate and compete in ways that ultimately enhance technology, health care, and consumer health and welfare.

ONC believes these criteria, as further elaborated in this report, will provide stakeholders with principled and practical guidance on information blocking. These criteria respect the legitimate economic interests of providers, developers, and other market participants; are narrowly tailored to the core public policy concerns that information blocking presents; and accommodate the difficult and highly circumstantial task of identifying information blocking and distinguishing it from other barriers to interoperability and health information exchange. These and other considerations are described below.

Distinguishing Information Blocking from Other Barriers to Interoperability and Health Information Exchange

Some kinds of conduct, though they interfere with the exchange or use of electronic health information, are unlikely to meet the criteria for information blocking. In particular, certain systemic barriers to interoperability and electronic health information exchange may cause persons or entities to act in ways that undermine effective information sharing for reasons that are beyond their control.

A major barrier to effective information sharing is the lack of coordination among many persons and entities that participate in or facilitate health information exchange. These coordination problems often stem from technical or practical challenges that are beyond the control of any individual actor. As a result, persons or entities may implement technical standards in inconsistent ways; adopt divergent privacy, security, or trust policies that govern how electronic health information is exchanged and used; or engage in other inefficient behaviors that inhibit or reduce opportunities to exchange and use electronic health information to improve care and care delivery.[18]

In general, these inefficient and uncoordinated behaviors do not raise information blocking concerns because they result not from a knowing and unreasonable interference but from larger, systemic barriers to interoperability and health information exchange—the kinds of barriers that the HITECH Act and other reforms directly seek to address. ONC's draft *Shared Nationwide Interoperability Roadmap*[19] describes steps that ONC and other stakeholders must take to overcome these and other challenges.

Conduct That Raises Information Blocking Concerns

In contrast to the behaviors described above, information blocking concerns arise when providers or developers knowingly engage in practices that are likely to interfere with exchange or use of electronic health information. In the absence of a reasonable justification, these practices are contrary to the public interest in promoting greater and more effective exchange and use of electronic health information to improve health and health care quality and efficiency.

---

[18] A similar lack of coordination exists among the states, which often employ different laws governing the privacy and security of health information and different network and governance approaches for statewide information exchange.

[19] *Roadmap*, *supra* n.11.

Practices that knowingly interfere with health information exchange are especially problematic when they prevent individuals from accessing their electronic health information or restrict providers and other authorized persons from exchanging basic clinical information[20] necessary for effective patient care. The sharing of this information is the focus of significant federal investments in health information exchange and the meaningful use of health IT and is essential to achieving the purposes of the HITECH Act.[21]

Available evidence and ONC's experience suggest that certain business, technical, and organizational practices are inherently likely to interfere with the exchange of electronic health information in ways that raise these serious information blocking concerns. These practices include but are not limited to:

- Contract terms, policies, or other business or organizational practices that restrict individuals' access to their electronic health information or restrict the exchange or use of that information for treatment and other permitted purposes.
- Charging prices or fees (such as for data exchange, portability, and interfaces) that make exchanging and using electronic health information cost prohibitive.
- Developing or implementing health IT in non-standard ways that are likely to substantially increase the costs, complexity, or burden of sharing electronic health information, especially when relevant interoperability standards have been adopted by the Secretary.
- Developing or implementing health IT in ways that are likely to "lock in" users or electronic health information; lead to fraud, waste, or abuse; or impede innovations and advancements in health information exchange and health IT-enabled care delivery.

Because of their inherent potential to interfere with health information exchange, these practices, when undertaken knowingly and without a reasonable justification, constitute information blocking.[22] Whether any reasonable justification exists will depend on the attendant facts and circumstances and require a careful consideration of the objective reasons for the practice; its likely impact on health information exchange; the extent to which it could have been reasonably avoided; and the extent to which it advances any countervailing interest.

Countervailing Interests

The HITECH Act seeks to promote the secure exchange and use of electronic health information not as an end in itself, but as a means to improving health and health care. While furthering the availability of electronic health information as needed for these purposes is a compelling interest, other important interests may justify certain controls over the exchange of electronic health information in appropriate circumstances. Such interests include protecting patient safety;[23] maintaining the privacy and security of individuals' health information;[24] and promoting competition and consumer welfare.[25]

---

[20] Such basic clinical information includes but is not limited to the common clinical data set and specific data elements described in the draft *Shared Nationwide Interoperability Roadmap*. *See Roadmap*, *supra* n.11.
[21] *See* Public Health Service Act §§ 3001(b)(2)–(3), 42 U.S.C. §§ 300jj–11(b)(2)–(3) (enumerating among the purposes of the HITECH Act efforts to advance patient safety, health care quality, and patient-centered care; and to reduce health care costs resulting from inefficiency, medical errors, inappropriate or duplicative care, and incomplete information).
[22] Some practices, such as restricting an individual's access to their electronic health information, may violate federal or state law.
[23] *Cf.* Public Health Service Act § 3001(b)(2), 42 U.S.C. § 300jj–11(b)(2).
[24] *Cf.* Public Health Service Act § 3001(b)(1), 42 U.S.C. § 300jj–11(b)(1).
[25] *Cf.* Public Health Service Act § 3001(b)(10), 42 U.S.C. § 300jj–11(b)(10).

The HITECH Act recognizes the need to protect the legitimate economic interests of providers, developers, and other market participants.[26] These economic interests are important because they provide incentives to innovate and compete to improve health care and health IT, which in turn benefits consumers and the health care system. Providers and developers who invest resources to develop and deploy more effective, interoperable health IT and health information exchange capabilities may not do so if they cannot realize a return on their investments. In addition, competition among developers as to how they price and deliver health IT and health information exchange services may reduce the costs of these technologies and provide more options for those who purchase and use them.

On the other hand, some business practices, though they may arguably advance legitimate individual economic interests, interfere with the exchange of electronic health information in ways that raise serious information blocking concerns. At some point, ONC believes that decisions to engage in such practices are unreasonable as against public policy, particularly when less restrictive alternatives exist and the economic benefits to consumers are outweighed by the costs to consumers of less effective and efficient health care.

The hypothetical scenarios in Appendix A illustrate how ONC would analyze and weigh these competing considerations in the context of specific, real-world fact patterns.

---

[26] Promoting "a more effective marketplace, greater competition, . . . , increased consumer choice, and improved outcomes in health care services" is one of the express purposes of a nationwide health IT infrastructure for health information exchange. *See* Public Health Service Act § 3001(b)(10), 42 U.S.C. § 300jj–11(b)(10).

III. DESCRIPTION OF KNOWN EXTENT OF INFORMATION BLOCKING

This section surveys available evidence of information blocking, including complaints and other anecdotes, relevant empirical data and research, and the accumulated knowledge and experience of ONC. While this evidence provides valuable insight into certain types of business practices and other conduct that raise information blocking concerns, it also has significant limitations. These limitations are discussed at the end of this section.

Anecdotal Evidence of Potential Information Blocking

ONC's understanding of information blocking is informed in part by a substantial body of complaints and other anecdotal evidence. In 2014, ONC received approximately 60 unsolicited reports of potential information blocking. In addition, ONC staff reviewed many additional anecdotes and accounts of potential information blocking found in various public records and testimony, industry analyses, trade and public news media, and other sources. ONC staff also invited stakeholders to share their experiences with information blocking. In-person discussions and phone calls were conducted with Regional Extension Centers (RECs)[27] and a number of other industry sources, including consumers, health care professionals and executives, health IT implementers, EHR technology and other health IT developers, state and regional health information exchange organizations (HIEOs), health care and health IT researchers, state and local government officials, and former ONC grantees.

Most complaints of information blocking are directed at health IT developers. Many of these complaints allege that developers charge fees that make it cost-prohibitive for most customers to send, receive, or export electronic health information stored in EHRs, or to establish interfaces that enable such information to be exchanged with other providers, persons, or entities. Some EHR developers allegedly charge a substantial per-transaction fee each time a user sends, receives, or searches for (or "queries") a patient's electronic health information. EHR developers may also charge comparatively high prices to establish certain common types of interfaces—such as connections to local labs and hospitals. Many providers also complain about the costs of extracting data from their EHR systems for their own use or to move to a different EHR technology.

Reports from RECs and other sources confirm wide variation in the fees developers charge for these products and services. Some of this variation likely reflects differences in developers' costs resulting from different technology architectures and service models, different capabilities and levels of service that developers offer, and different ways in which developers choose to distribute these and other costs across customers. However, these factors do not adequately explain all of the variation in prices that have been reported to ONC. There are indications that at least some developers may be engaging in opportunistic pricing practices[28] or charging prices that are designed to deter connectivity or exchange with competing technologies or services.

[27] Regional Extension Centers provide on-the-ground technical assistance to individual and small provider practices and public and critical access hospitals.

[28] Certain characteristics of EHR technology markets—in particular, high costs to switch to different technologies and a lack of up-front information about the relative costs, capabilities, and total cost of ownership of health IT products and services—likely enable some EHR developers to engage in opportunistic pricing and other conduct that exploits locked-in customers. These concerns are described at length in section IV of this report in connection with the need for greater transparency in health IT markets.

Complaints that developers are engaging in information blocking often allege a combination of one or more contractual terms,[29] technology design decisions, and other business practices that restrict users of a developer's technology from exchanging health information with users of competing technologies or services. ONC has received many complaints alleging that some EHR developers either prohibit or make it unnecessarily difficult or expensive for their customers to connect to third-party health IT modules, even when such modules have been certified by ONC and would enable customers to connect and share electronic health information with a wider network of providers and other exchange partners. For example, EHR developers may prohibit customers from selecting an ONC-certified Health Information Service Provider (HISP) of their choosing, requiring instead that customers use only the developer's own HISP and other exchange platform and services. This is problematic when the developer's own HISP and exchange platform are designed or deployed in such a way that they prevent users from meeting desired technical or trust requirements necessary to connect and exchange information with other providers and entities, including some state and regional entities that facilitate electronic health information exchange across diverse providers, technologies, and geographies.

Some complaints and anecdotes allege that developers are preventing the exchange of health information with competitors or with specific providers. A recurring allegation is that certain EHR developers refuse to establish interfaces or connections with certain technologies or entities (or will do so only on terms so onerous that they amount to a refusal for all practical purposes). Some of these developers cite security concerns and business justifications for these practices, while others provide no justification or, in some cases, appear to acknowledge a strong preference not to exchange information using federally adopted standards and to instead drive more users to exchange information using proprietary platforms and services.

Health care providers have also been accused of information blocking. A common charge is that some hospitals or health systems engage in information blocking to control referrals and enhance their market dominance. Providers have cited many reasons for constraining access to electronic health information. The most common reason cited is to comply with privacy and security requirements. Such constraints are not information blocking insofar as they are consistent with the requirements and policies established by federal and state law that protect patients' electronic health information. But it has been reported to ONC that privacy and security laws are cited in circumstances in which they do not in fact impose restrictions. For example, providers may cite the HIPAA Privacy Rule as a reason for denying the exchange of electronic protected health information for treatment purposes, when the Rule specifically permits such disclosures.

ONC has also received complaints or anecdotes of potential information blocking that allege coordination between developers and their provider customers to restrict exchange with unaffiliated providers. For example, a developer may have the requisite trust relationships and technological capabilities to exchange secure messages using the federal Direct standard with a large network of providers. But the developer and provider may implement this capability so as to restrict the exchange of information to physicians who are members of the provider's care network (e.g., by preventing users from entering a recipient's Direct email address and requiring instead that users select recipients from a pre-populated drop-down list).

[29] Examples of contractual restrictions include express prohibitions, penalty clauses, and cancellation of warranty clauses.

Descriptions of information blocking in public records and testimony, and from industry sources, raise many of the same concerns reported to ONC. Several observers have alleged that providers and developers are imposing artificial constraints on health information exchange.[30] These constraints may include contractual restrictions or involve other business practices aimed at preventing information from being exchanged.[31] Other cited examples of information blocking include the use of proprietary data formats to lock customers into systems, failing to publish application programming interfaces (APIs) for data elements required to be exchanged under the EHR Incentive Programs, and charging differential fees unrelated to increased costs of exchanging information.[32] In addition to these specific types of business practices, certain types of strategic business choices or ways of doing business have been characterized as information blocking by some commentators.

Many of these concerns were voiced during a March 2014 public workshop hosted by the Federal Trade Commission (FTC) that examined emerging trends in the rapidly changing health care industry.[33] The workshop included a session that explored recent developments and competition issues in health IT markets. Several panelists and commentators expressed concerns about developers or providers who restrict health information exchange or data portability. For example, some health IT contracts may "restrict a health care provider's ability to use data contained within an EHR,"[34] require health care provider staff to complete costly developer-imposed training or "certification" requirements before they are allowed to extract and use information, or impose "access and use agreements" that restrict a provider's ability to "engage a third party to assist with extracting and using data to benefit patients."[35] Some developers also purportedly make it difficult for providers to transport their patients' electronic health information in the event that the provider chooses to switch to a competitor's EHR technology, or charge "additional fees to allow providers to extract patient data from their systems, even though the marginal cost of providing that data is small."[36] These business practices, combined with the expense of implementing and training staff on new systems, make it very costly and difficult for providers to switch to other technologies, even when they are unsatisfied with the performance of their existing technology.

Panelists and commentators also raised concerns that providers and developers may be engaging in information blocking as a means of "locking in" providers and consumers to rigid technologies and information sharing networks that reinforce the market dominance of established players and prevent

---

[30] Reps. D. Black and M. Honda, *July 11, 2013 letter to M. Tavenner and F. Mostashari*, available at http://op.bna.com/hl.nsf/id/kcpk-99mnkx/$File/711EHRletter.pdf. *Cf.* Health IT Now Coalition, Submission to FTC Health Care Workshop, Project No. P131207, http://www.ftc.gov/system/files/documents/public_comments/2014/03/00045-88879.pdf (reciting and elaborating on Black and Honda's definition); Joel White, *What is Information Blocking?,* http://www healthitnow.org/what-is-information-blocking/ (elaborating further).

[31] Black and Honda, *supra* n.30 (citing as an example of information blocking "contracts that block information exchange between electronic health record systems").

[32] White, *supra* n.30. *See also* Arthur Allen, *Doctors Say Data Fees Are Blocking Health Reform*, POLITICO.COM (Feb 23, 2015), available at http://www.politico.com/story/2015/02/data-fees-health-care-reform-115402 html.

[33] FTC, Health Care Workshop, Project No. P131207 (Mar 2014) (hereinafter "FTC Workshop"). Transcripts and public comments are available at http://www ftc.gov/news-events/events-calendar/2014/03/examining-health-care-competition.

[34] FTC Workshop, *supra* n.33, Submission #00187 (The Advisory Board Company).

[35] *Id.*

[36] FTC Workshop, *supra* n.33, Submission #00045 (Health IT Now Coalition).

competition from more innovative technologies and services.[37] Customers who become "locked in" to a particular technology may find it prohibitively expensive to switch to new technologies (or different delivery networks) that offer superior value, capabilities, and opportunities for delivering higher quality and more efficient care. Some panelists and commentators suggested that provider and developer business models based on "walled gardens"—closed information sharing networks often based on expensive and proprietary health IT solutions adapted to the needs of existing health care delivery systems—were fundamentally incompatible with the shift towards new care delivery models that reward quality and value. [38]

Empirical Data and Research on Health Information Exchange

Empirical data and research on electronic health information exchange capabilities and trends provide important context for analyzing anecdotal evidence and understanding the nature and extent of information blocking.

ONC relies on several types of data to assess national progress and conducts its own analyses on health information exchange and interoperability. These include national surveys (hospitals and office-based physicians), data collected through the EHR Incentive Programs, data reported by RECs, and case studies performed by contracted evaluators of HITECH programs.

Through national surveys, ONC monitors the adoption of exchange functionalities over time. In particular, ONC has identified variation in health information exchange capabilities between health care provider types, regions, and EHR developers. For example, ONC has shown that there is large variation among physicians' capabilities to exchange clinical summaries with other providers by their EHR developer.[39] This suggests that health information exchange may be easier with some EHR developers than others. ONC has also shown that large hospital systems are more likely to have greater health information exchange capabilities than small and single practice providers.[40]

A growing body of research has focused on the degree to which hospitals and hospital systems exchange electronic health information with competing or unaffiliated providers. Evidence shows that larger hospital systems are more likely to exchange electronic health information internally, but are less likely to exchange electronic health information externally with competing hospitals and unaffiliated providers.[41] This in turn reduces the likelihood that these other providers will exchange information.[42] Hospitals that have invested significant resources internally to deliver more valuable care may also be less likely to exchange electronic health information with unaffiliated providers.[43] Evidence also shows that for-profit

---

[37] *See* FTC Workshop, *supra* n.33, Tr. (Mar 21, 2014) at 118, 148–49; Tr. (Mar 22, 2014) at 131–32; Submission #00141 (athenahealth, Inc.); Submission #00161 (Verizon Communications, Inc.); Submission #00187 (The Advisory Board Company); Submission #00045 (Health IT Now Coalition).
[38] *Id.*
[39] Michael Furukawa, Vaishali Patel, Chun-Ju Hsiao, Julia Adler-Milstein, & Ashish Jha, *Despite Substantial Progress In EHR Adoption, Health Information Exchange and Patient Engagement Remain Low In Office Settings*, 9 HEALTH AFFAIRS 1672 (2014).
[40] Michael Furukawa, Vaishali Patel, Dustin Charles, Matthew Swain, & Farzad Mostashari, *Hospital Electronic Information Exchange Grew Substantially in 2008-12*, 8 HEALTH AFFAIRS 1346 (2013).
[41] Amalia Miller & Catherine Tucker, *Health Information Exchange, System Size and Information Silos*, 33 J. HEALTH ECON. 28 (2014).
[42] *Id.*
[43] *Id.*

hospitals are less likely than non-profit hospitals to exchange electronic health information externally, as are hospitals that do not have significant market share or operate in less concentrated (more competitive) markets. [44]

These results suggest that business and competitive motivations influence whether hospitals and hospital systems choose to exchange electronic health information with unaffiliated providers. Moreover, larger hospitals and hospital systems have the ability to influence health information exchange by other providers in their communities. These findings lend some support to anecdotal evidence suggesting that some hospitals or health systems may be engaging in information blocking to control referrals or to otherwise enhance their market dominance.

Where Knowledge of Information Blocking is Limited and How to Resolve

Available evidence provides valuable insight into information blocking, including certain general types of behaviors and actors that raise information blocking concerns. However, this evidence has significant limitations that prevent ONC from confirming individual cases of information blocking.

Identifying and confirming specific instances of information blocking is a difficult and highly fact-specific task. As the discussion above illustrates, ONC receives many complaints that allege business practices or other conduct that raises information blocking concerns. Sometimes the allegations in these complaints can be corroborated with information from other sources. But even so, this evidence is not balanced with information from the accused party's perspective, including information that may provide a reasonable justification for the alleged interference with health information exchange. ONC also lacks access to the kind of detailed price and cost data, contractual language, technical documentation, and other evidence necessary to objectively determine whether conduct meets the definition and criteria for information blocking established in section II of this report. ONC's ability to require or effect the disclosure of this information is in many respects limited. Section IV of this report describes steps that ONC is taking or has proposed to take to increase the availability of this information, to the extent possible, given limitations of current programs and authorities.

Empirical data on information blocking is also limited at present. There is little quantitative data available with which to reliably identify and measure the extent of information blocking. Currently, ONC can assess the health information exchange capabilities associated with different types of providers or with certain types of market characteristics; but this information does not enable ONC to pinpoint and confirm actual cases of information blocking or reliably estimate the extent of such conduct. In particular, ONC lacks methods and data to precisely determine why a provider is not exchanging when they should have the capability to do so. Newer versions of national surveys are expected to collect a richer set of data on barriers to health information exchange that may provide deeper insights into information blocking. However, these surveys have significant limitations: they do not have perfect response rates; their results are self-reported; and they are conducted on an annual basis, which restricts the timeliness and relevance of results. Overall, available data enables ONC to identify areas where there is or could be pressure to interfere with health information exchange, but does not allow us to identify where exactly information blocking occurs.

---

[44] Julia Adler-Milstein & Ashish Jha, *Health Information Exchange Among U.S. Hospitals: Who's In, Who's Out, and Why?*, 2 HEALTHCARE 26 (2014).

As part of the draft *Shared Nationwide Interoperability Roadmap*, ONC has identified a number of measurement gaps in monitoring progress related to interoperability. To fill these gaps, ONC is considering additional sources of data from key entities that enable health information exchange and interoperability, such as HIEOs, HISPs, and health IT developers. Such entities can provide information on the volume of exchange activity, as well as the availability and usage of exchanged data. Metrics to monitor information blocking specifically could be a part of this measurement strategy. For example, Direct Trust has reported transaction-based data on key metrics related to the volume of exchange activity based upon data provided by its participants.[45] However, this represents a subset of all the exchange activity that is enabled nationwide, and it is self-reported by the entities participating in Direct Trust.

ONC's collaborations with federal partners may also yield information and data that could be relevant for analyzing information blocking. For example, in the *Federal Health IT Strategic Plan 2015-2020,* a number of federal partners have committed to reporting on interoperability. ONC has also developed collaboration with FTC to identify market barriers to exchange and interoperability.[46] Federal agencies, such as the Agency for Healthcare Research & Quality (AHRQ), already support research related to electronic health information exchange and interoperability and will continue to do so. ONC will coordinate with these agencies to ensure that information blocking is considered.

To fill gaps in empirical data and research, ONC may need to commission market reports and other data collection activities on electronic health information exchange. Such data collection could include conducting or commissioning additional surveys or creating a public reporting process with structured questions through which complaints of information blocking can be submitted. These and other activities would allow for a more focused examination of barriers to health information exchange and interoperability, including information blocking. However, such activities would be contingent on available funding, authority, and compliance with information collection requirements and other applicable laws.

[45] Exemplar Health Information Exchange Governance Entities Program (Program) Funding Opportunity Announcement. http://www.healthit.gov/policy-researchers-implementers/exemplar-hie-governance-entities-program.

[46] Tara Isa Koslov, Markus Meier, and David R. Schmidt, *Promoting Healthy Competition in Health IT Markets*, http://www.ftc.gov/news-events/blogs/competition-matters/2014/10/promoting-healthy-competition-health-it-markets (Oct 7, 2014).

IV. CHARACTERISTICS OF A COMPREHENSIVE STRATEGY TO LIMIT INFORMATION BLOCKING

Need for a Comprehensive Approach

ONC believes that information blocking can be most effectively addressed through a comprehensive approach, consisting of both targeted actions to deter and remedy information blocking as well as broader strategies that address the larger context in which information blocking occurs.

Many actions that do not meet the criteria for information blocking still interfere with the effective exchange and use of electronic health information. In addition, a variety of systemic barriers to interoperability and health information exchange also impede progress towards more meaningful information sharing. Addressing these broader challenges will require, among other things:

- Continued public and private sector collaboration to develop and drive the consistent use of standards and standards-based technologies that enable interoperability.
- Establishing effective rules and mechanisms of engagement and governance for electronic health information exchange.
- Fostering a business, clinical, cultural, and regulatory environment that is conducive to the exchange of electronic health information for improved health care quality and efficiency.
- Clarifying requirements and expectations for secure and trusted exchange of electronic health information, consistent with privacy protections and individuals' preferences, across states, networks, and entities.

The recently published draft *Shared Nationwide Interoperability Roadmap*[47] represents ONC's continued commitment to understanding and overcoming these complex challenges, together with industry, government, and the health IT community. Continuing to address and solve these challenges will be among the most important actions the federal government can take to help prevent information blocking and ensure that the nation's health IT and health care vision is fulfilled.

Targeted Actions to Address Information Blocking

ONC believes that, as part of this comprehensive approach, specific actions can and should be taken to address information blocking. ONC is already taking a variety of actions to target, deter, and remedy information blocking and will coordinate with federal agencies that have the ability to investigate and take action against certain types of information blocking. These strategies and actions are described in detail below.

Strengthen In-the-field Surveillance of Health IT Certified by ONC

ONC may be able to address some types of information blocking through the ONC HIT Certification Program.[48]

The ONC HIT Certification Program certifies health IT's conformance to specific standards and functionality adopted by the Secretary via rulemaking, including technical standards, implementation

[47] *Roadmap*, *supra* n.11.
[48] See Appendix B for an overview of the ONC HIT Certification Program.

specifications, and certification criteria that specify particular capabilities that health IT must demonstrate to be issued a certification. Many of these certification requirements are aimed at enabling interoperable information sharing.

The ONC HIT Certification Program vests responsibility for certifying and ensuring ongoing conformance of health IT in ONC-Authorized Certification Bodies (ONC-ACBs). ONC-ACBs must provide proactive and reactive surveillance of health IT they certify in order to maintain their accreditation and authorization to issue certifications on behalf of ONC. If an ONC-ACB can substantiate a non-conformity, either as a result of surveillance or repeat product conformance testing, the ONC-ACB in collaboration with ONC has several corrective action options, which include: (1) the continuation of the certification under specified conditions (e.g. increased surveillance); (2) suspension of the certification pending remedial action by the developer; and (3) termination of the certification.

Certain types of information blocking may compromise the performance of health IT capabilities certified under the ONC HIT Certification Program. If the result of actions by the health IT's developer, such information blocking could result in corrective action, up to and including the termination of the certification issued to the developer's health IT. For example, developers of certified health IT products and services may impose contractual or other restrictions on the ability of users to access or use capabilities required for certification, such as the capability to send an electronic patient care summary to another provider[49] or export a basic set of electronic health information for a patient.[50] These restrictions on health IT's certified technical capabilities would risk the technology's certification and, if not corrected, could result in suspension or termination of the health IT's certification.

In the Health Information Technology Certification Criteria, Base Electronic Health Record Definition, and ONC Health IT Certification Program Modifications proposed rule (hereinafter "2015 Edition Certification Proposed Rule"),[51] ONC has proposed more aggressive surveillance requiring disclosure by developers of any limitations of the technology that may interfere with the ability of users to access or use certified health IT capabilities. The proposed rule would require ONC-ACBs to conduct more extensive "in-the-field" surveillance of certified health IT and to do so based on both complaints and a randomized sampling approach. The proposed rule also introduces additional corrective action procedures for certain types of non-conformance.

While these measures will assist ONC-ACBs to identify and address certain kinds of information blocking that interfere with the performance of certified health IT capabilities, many types of information blocking will remain beyond the reach of ONC-ACBs and the ONC HIT Certification Program. These limitations are explained subsequently under the heading "Gaps and Additional Areas for Consideration."

Constrain Standards and Implementation Specifications

ONC-ACB surveillance activities and other feedback from the field show that although certified health IT is often conformant with the criteria to which it was certified, there is still a substantial amount of permissible variability in the underlying required standards, unique clinical workflow implementations, and numerous types of interfaces to connect multiple systems. This variability has contributed to

[49] 45 C.F.R. § 170.314(b)(2) (Transitions of Care – Create and Transmit Summary Care Records). Last revised March 1, 2013.
[50] 45 C.F.R. § 170.314(b)(7) (Data Portability). Last revised May 8, 2013.
[51] 80 Fed. Reg. 16804 (Mar 30, 2015).

information sharing challenges and also creates opportunities for developers or health IT implementers to erect unnecessary technical barriers to interoperability and electronic health information exchange.

ONC is actively working with all stakeholders to improve interoperability and information sharing. In the future, ONC will improve information sharing and reduce information blocking by working with standards developing organizations to further constrain standards and their corresponding implementation guides and develop more robust technical testing tools. These actions would reduce standards optionality within the certification rules so that greater interoperability is achieved. They would also enhance conformance testing, both in the controlled testing environment in which health IT is initially tested for certification, and "in the field" during post-implementation surveillance and testing. The latter is especially important for verifying that users of certified health IT are able to successfully access and implement certified capabilities that enable data portability and health information exchange.

Promote Greater Transparency in Certified Health IT Products and Services

One of the most effective ways to reduce information blocking is to promote transparency in the health IT marketplace. Providing customers with more reliable and complete information about health IT products and services would make developers more responsive to customer demands and help ameliorate market distortions that enable developers to engage in certain opportunistic and other behavior that raises serious information blocking concerns.

Today, many providers and other purchasers and licensees of health IT products and services lack reliable information about the true costs and limitations of these technologies.[52] As a result, they may be unable or less likely to purchase or license products and services that best meet their needs. Further, poor purchasing or licensing decisions are often magnified by the extensive cost and resources required to implement health IT.[53] Having made these investments, providers may be financially and otherwise unable to switch to superior technologies that offer greater interoperability, health information exchange capabilities, and other features. These switching costs make it easier for developers to engage in information blocking without losing existing customers. A lack of transparency in the marketplace meanwhile increases incentives for developers to engage in practices that increase "lock-in" of customers and information, thereby exacerbating the information blocking problem. In this climate, reliable up-front

[52] Feedback from stakeholders suggests that many purchasers still have limited access to certain types of information necessary to accurately assess the potential costs, benefits, limitations, and trade-offs of alternative technologies and solutions. *See, e.g.*, Jodi G. Daniel & Karson Mahler, *Promoting Competition to Achieve Our Health IT and Health Care Goals* (Oct. 7, 2014), http://www healthit.gov/buzz-blog/health-information-exchange-2/promoting-competition-achieve-healthit-health-care-goals/. This is especially true of smaller providers who do not have the time, resources, or expertise to conduct extensive market research. *See, e.g.*, Kelly Devers, Arnav Shah, & Fredric Blavin, *How Local Context Affects Providers' Adoption and Use of Interoperable Health Information Technology: Case Study Evidence from Four Communities in 2012 (Round One)* (2014), at 7 (describing significant challenges faced by smaller providers dealing with certified EHR vendors, including "understanding vendor contracts that were very complex."). Health IT customers and industry observers describe a marketplace that is opaque and in which purchasers often lack up-front information about the products and services they purchase or license. For example, the American Medical Association (AMA) has expressed concern on behalf of its members about "the lack of transparency in EHR contracts," which "may be unclear or fail to itemize specific expenses." FTC Workshop, *supra* n.33, Submission #00151 (American Medical Association). The AMA further noted that while ONC has taken steps to promote greater contract transparency, "broad discretion and uncertainty" persists in health IT markets. *Id.*

[53] Implementation costs include not only the costs of purchasing or licensing health IT but also those associated with installation and configuration, training, integration of existing legacy IT systems, interface development, and changes to clinical and administrative workflows, among other costs.

information about health IT products and services is all the more important to ensure that developers are accountable and responsive to customers' preferences.

ONC's 2015 Edition Certification Criteria Proposed Rule[54] would introduce new and significantly enhanced transparency and disclosure obligations for developers. Developers would be required to disclose the limitations and additional types of costs associated with health IT—whether to demonstrate meaningful use objectives or measures or for any other purpose within the scope of the health IT's certification—that could interfere with the use of health IT and health information exchange capabilities certified by ONC. These disclosure obligations would be subject to in-the-field surveillance by ONC-ACBs. Developers would also publicly attest to voluntarily providing that same information to any person who requests it.

Notwithstanding these important efforts, the persistent lack of transparency and access to reliable information about health IT products and services, including for electronic health information exchange, is a significant problem that not only causes and exacerbates information blocking but substantially impairs the efficient functioning of health IT markets. While ONC is pursuing all avenues to enhance transparency and require more meaningful disclosure of developer business practices that block information, ONC's ability to address this problem is limited in several respects. These limitations are elaborated in the discussion of "Gaps and Additional Areas for Consideration" below.

Establish Governance Rules That Deter Information Blocking

Many types of information blocking could be mitigated by encouraging or requiring providers, developers, and others that facilitate the exchange of electronic health information to adhere to certain basic expectations related to the availability and sharing of information for purposes of patient care. As described in the draft *Shared Nationwide Interoperability Roadmap*,[55] ONC intends to specify a coordinated governance framework and process for nationwide health information interoperability that includes: (1) common "rules of the road" for trust and interoperability among providers, developers, and other entities that facilitate electronic health information exchange; and (2) a mechanism for recognizing entities that comply with these common rules.

These "rules of the road," which will first focus on interoperability of a common clinical data set for purposes of treatment, will adhere to a number of important principles. Two of these principles in particular address key business practice issues that are among the most common complaints of information blocking received by ONC:

> ***Share Protected Health Information.*** Entities that hold data or facilitate exchange would be expected to adhere to a principle that discourages them from erecting unnecessary policy, business, operational, or technical barriers to information sharing for patient care, care coordination, and other purposes that are consistent with applicable law, professional ethical standards, and patient preferences.
>
> ***Open Exchange.*** Entities that facilitate exchange (e.g., EHR developers, HISPs, HIEOs) would be held to an expectation of neutrality and discouraged from erecting barriers to information sharing based solely on favoritism toward specific business partners. For instance, a developer

[54] 80 Fed. Reg. 16804 (Mar 30, 2015).
[55] *Roadmap*, *supra* n.11.

that has health information exchange applications would be expected not to engage in business practices that prevent a user from using health information exchange applications developed by the developer's competitors.

Adherence to these basic principles would discourage providers, developers, and other entities from erecting many artificial barriers that currently impede exchange. For example, developers adhering to these principles could not impose costs or fees that would make the electronic exchange of clinical information with users of competing health IT products or services cost-prohibitive, or render it cost-prohibitive for a provider to comply with a patient's right of electronic access.

ONC is examining available approaches for establishing an effective governance mechanism that will hold actors accountable to these principles and other rules for trust and interoperability. As part of this process, ONC will keep Congress informed about available approaches and any additional authorities that may be needed.

Work in Concert with the HHS Office for Civil Rights to Improve Stakeholder Understanding of the HIPAA Privacy and Security Standards Related to Information Sharing

The success of electronic health information exchange is heavily dependent upon patients recognizing and being willing to participate in the sharing of their health information. As key agents of trust for patients, health care providers are responsible for maintaining the privacy and security of their patients' health information.

As outlined in the draft *Shared Nationwide Interoperability Roadmap*,[56] ONC will work in concert with the HHS Office for Civil Rights (OCR) to improve health IT stakeholders' understanding of the HIPAA Rules and how they support interoperable exchange by permitting disclosures of protected health information (PHI) for treatment, payment, and health care operations (TPO). To achieve interoperability, all entities regulated by the HIPAA Rules must understand the circumstances under which the Rules permit the sharing of PHI. With improved understanding, stakeholders will be able to exchange electronic health information appropriately with greater confidence. Improved understanding also would decrease the likelihood that health care providers and health plans fail to respond appropriately when individuals exercise their legal right under the HIPAA Rules to access their own health information.

The federal government, through OCR, will consider where additional guidance and outreach may be needed to help stakeholders understand how the HIPAA Privacy Rule permits PHI to be exchanged (disclosed) for TPO without consent or authorization. ONC will also work to help align stakeholder policies with the HIPAA Rules.

The HIPAA Rules, however, are not the only applicable rules that protect privacy; states can and do enact laws that are more privacy protective. Unfortunately, the resulting legal privacy patchwork is not easily understood by implementers. As a result, some providers or other persons or entities may mistakenly or even intentionally misinterpret or misrepresent state privacy laws as prohibiting the sharing (disclosure) of electronic PHI—either with individuals directly or with other health care providers that an individual has designated—in circumstances when federal and state law permit such disclosure. This misapplication of privacy law may result in the denial of individuals' access to their electronic health information, prevent individuals from directing a health care provider to send their health information to another health

[56] *Roadmap, supra* n.11.

care provider of their choice (such as one that is not affiliated with the originating provider), or prevent or deter providers from sharing individuals' health information with other entities for legitimate purposes allowed under applicable law.[57] This behavior is of increasing concern to ONC given that a growing number of providers are adopting and demonstrating the meaningful use of certified health IT and should therefore have the capability to disclose PHI to individuals in electronic form[58] and to exchange this information electronically with other providers.

Coordinate With the HHS Office of Inspector General (OIG) and CMS Concerning Information Blocking in the Context of the Federal Anti-kickback Statute and Physician Self-referral Law

Certain federal laws designed to prevent fraud and abuse in connection with federal health care programs restrict many types of transactions and financial relationships involving health IT products and services. For example, the federal anti-kickback statute (AKS) [59] makes it a criminal offense to knowingly and willfully offer, pay, solicit, or receive any remuneration to induce or reward referrals of items or services reimbursable by a federal health care program.[60] Thus, the offer, provision, solicitation, or receipt of health IT products or services may constitute illegal remuneration under the AKS.

The physician self-referral law[61] prohibits, among other things, a physician from making referrals for certain designated health services payable by Medicare to an entity with which he or she (or an immediate family member) has a financial relationship, unless an exception applies. Therefore, certain arrangements involving health IT may also give rise to illegal referrals (or illegal claims for reimbursement) under the physician self-referral law.

Depending on the circumstances and the law at issue, violations of these federal statutes can result in severe civil and criminal liability, civil monetary penalties, exclusion from federal health care programs, and additional liability under the federal False Claims Act. There is an AKS safe harbor[62] and an exception to the physician self-referral law[63] that protect certain donation arrangements involving interoperable electronic health records software or information technology and training services. Protection under the AKS or physician self-referral law is available only when all of the applicable conditions of the safe harbor or exception, respectively, are met. The conditions of the safe harbor and exception are similar. One of those conditions requires that "the donor (or any person on the donor's behalf) does not take any action to limit or restrict the use, compatibility, or interoperability of the items or services with other electronic prescribing or electronic health records systems (including, but not limited to, health information technology applications, products, or services)."[64] Engaging in information blocking can cause a donation arrangement to fall outside of the safe harbor or exception.[65] In connection with the AKS, donation arrangements that fail to meet the above-described condition because the donor or

[57] 45 C.F.R. § 164.506(c).
[58] 45 C.F.R. § 170.314(e)(1). Meaningful Use core measures include providing patients with the ability to view online, download and transmit their health information within four business days of the information being available to the eligible professional.
[59] Section 1128B(b) of the Social Security Act, codified at 42 U.S.C. § 1320a–7b(b).
[60] *See id.*
[61] Section 1877 of the Social Security Act, codified at 42 U.S.C. § 1395nn.
[62] 42 C.F.R. § 1001.952(y).
[63] 42 C.F.R. § 411.357(w).
[64] 42 C.F.R. § 1001.952(y)(3); see also, 42 C.F.R. § 411.357(w)(3).
[65] For examples of arrangements that may not meet this condition of the safe harbor and exception, *see* 78 Fed. Reg. 79202, 79213 and 78 Fed. Reg. 78751, 78762-3.

someone on the donor's behalf (including the recipient) took an action to limit or restrict interoperability would be suspect under the AKS as they would appear to be motivated, at least in part, by a purpose of securing federal health care program business.[66] If the physician self-referral law is implicated and no exception is met, then the law is violated.

ONC will coordinate with OIG and CMS concerning information blocking in the context of the AKS and physician self-referral laws.

Refer Illegal Business Practices to Appropriate Law Enforcement Agencies

In limited circumstances, some types of information blocking may violate state or federal law. ONC will provide assistance where appropriate to help federal and state law enforcement agencies identify and investigate such conduct.

Within HHS, ONC's Chief Privacy Officer will work to identify and refer to OCR for investigation information blocking and other business practices that may violate the HIPAA Rules. Similarly, as discussed above, ONC will coordinate with OIG and CMS concerning information blocking in the context of the AKS and physician self-referral law.

ONC will also support other state and federal law enforcement agencies to investigate potentially unlawful information blocking. For example, ONC coordinates closely with FTC's Bureau of Competition and Bureau of Consumer Protection to monitor health IT-related business practices that could implicate federal antitrust or consumer protection laws. ONC will continue to assist FTC to identify business practices that could harm competition or consumers. In consultation with FTC, ONC will also assist other law enforcement agencies, such as the Department of Justice (DOJ) and state attorneys general, who enforce relevant competition and consumer protection laws.

It is important to recognize that these laws were not enacted to specifically address most information blocking. As a result, investigation and enforcement of information blocking occurs only in relatively rare instances in which such conduct implicates other concerns that existing laws were designed to address. The implications of this significant limitation are described below in connection with the discussion of "Gaps and Additional Areas for Consideration."

Work with CMS to Coordinate Health Care Payment Incentives and Leverage Other Market Drivers to Reward Interoperability and Exchange and Discourage Information Blocking

Evolving health care payment from a volume to value based system could play a significant role in preventing information blocking.

Providers paid primarily on a fee-for-service basis have incentives not to exchange electronic health information outside their organizations because increased coordination of care can result in reduced volume of billable services (including duplicate and inappropriate services). Under new "value-based payment" programs, however, providers are increasingly reimbursed based on the health outcomes of individuals and the degree to which providers can reduce the total cost of care while improving health care quality and the patient experience. These value-based purchasing programs strengthen the business imperative to adopt common standards and exchange information across the care continuum to provide

[66] 78 Fed. Reg. 79213.

more coordinated and effective care. The increased efficiency from sharing data can increase providers' revenue. Under value-based payment, the technical and legal costs associated with the exchange of data would be viewed as necessary investments to increase revenue, while also maintaining or improving quality of care.

Over the past several years, the public and private sector alike have made progress toward changing the way health care is paid for, laying the groundwork for a value-based and person-centered health system. In January 2015, HHS announced new goals for moving Medicare payments from rewarding volume to rewarding value. Specifically, HHS set a goal of tying 30 percent of Medicare fee-for-service payments to quality or value through alternative payment models by 2016 and 50 percent by 2018.[67] As HHS continues to test and advance new models of care that reward providers for outcomes, it will help to create an environment where interoperability makes business sense. Additional policy levers across the public and private sector could also be leveraged to encourage interoperable health IT, including: 1) new incentives to adopt and use interoperable health IT systems to create additional demand for interoperability; and 2) requirements/penalties that raise the costs of not moving to interoperable health IT systems.[68]

Promote Competition and Innovation in Health IT and Health Care

Over the past year ONC and FTC have enhanced their collaboration to advance a shared commitment to promoting competition in health IT markets so that health IT is a driver of quality and value in health care.

This collaboration is especially important for addressing information blocking. In developing strategies and actions to address information blocking and other barriers to interoperability and health information exchange, ONC is mindful that successful implementation of the HITECH Act and the ACA's market-based reforms requires that health IT and health care markets function efficiently and foster innovation in technology and health care services. While ONC's focus is on expanding access to health information for all stakeholders, this cannot happen if market participants lack the necessary incentives to innovate new technologies and ways of delivering care.

The goals of advancing health information exchange and promoting competition and innovation are broadly compatible and will in most cases be aligned. ONC and FTC routinely share industry knowledge and expertise to better understand health IT and health care market dynamics and how these dynamics can both influence and be influenced by the success of federal health IT policies and programs. FTC has acquired deep expertise in health IT markets and competition, which, combined with its longstanding health care industry experience and unique range of research and advocacy tools, enables it to provide valuable guidance to ONC as it formulates market-based policies and approaches to advance interoperability and exchange. As ONC considers potential approaches to deter and remedy information blocking, it will seek input from FTC staff to ensure that any additional government intervention in health IT markets does not unnecessarily suppress competition or innovation and is narrowly tailored to remedying information blocking and removing other barriers and impediments to interoperability and health information exchange.

---

[67] *See supra* n.6.

[68] The draft *Shared Nationwide Interoperability Roadmap* describes efforts across HHS and the public and private sectors to pursue policy and funding levers that create the business imperative for interoperability. *See Roadmap*, *supra* n.11 at 37–44.

Gaps and Additional Areas for Consideration

The strategies and targeted actions outlined above will help deter and reduce the impact of information blocking. However, a comprehensive approach to this problem will require overcoming a number of significant gaps in current knowledge, programs, and authorities that currently limit the ability of ONC and other federal agencies to effectively target, deter, and remedy this conduct, even though it frustrates public policy. ONC believes that congressional action will likely be needed to address many of these gaps, which are described in detail below.

Limited Evidence and Knowledge of Information Blocking

ONC's industry knowledge and sources provide valuable insight into business practices and other conduct that may raise information blocking concerns. However, ONC and other federal agencies currently have limited ability to investigate and confirm specific instances of information blocking and cannot accurately estimate where and to what extent providers and developers are engaging in this practice.

Identifying information blocking is a difficult and highly fact-specific task that requires access to detailed and often sensitive information about provider or developer business, technical, and organizational practices. For example, where a developer engages in pricing or contractual practices that interfere with the exchange or use of electronic health information, evidence as to the developer's actual costs, prices, business model, and technology design decisions is necessary to determine whether the interference has any reasonable justification, and thus whether it rises to the level of information blocking.

ONC has no authority to require providers to produce relevant information (such as contracts with developers) and may have limited ability to require developers to produce this information outside the context of the ONC HIT Certification Program. ONC-ACBs may be able to investigate some types of information blocking through in-the-field surveillance of technology certified under the ONC HIT Certification Program. However, the focus of the ONC HIT Certification Program is to assess health IT's conformance to specific technical standards and capabilities.[69] While some types of information blocking may implicate these technical standards and capabilities, most allegations of information blocking involve business practices and other conduct that interferes with the exchange of electronic health information despite the availability of standards and certified health IT capabilities that enable this information to be shared. Most of these business practices and conduct are beyond the current scope of the ONC HIT Certification Program and may exceed the capacity of ONC-ACBs to effectively investigate. Moreover, for reasons discussed below, there is no basis for any other federal agency to investigate and develop evidence of these practices except in the relatively few circumstances in which such conduct violates some current provision of federal law.

A comprehensive strategy to address information blocking requires reliable evidence and knowledge with which to confirm and respond to individual cases of information blocking; better understand where and to what extent this conduct is occurring; and develop effective strategies and policies that target and address its root causes. Given the limitations above, better knowledge and access to evidence will be necessary to develop a comprehensive strategy and effective policies to target and address information blocking.

[69] See Appendix B.

Limitations of Certification for Addressing Information Blocking by Developers

Congress has urged ONC to leverage its certification authorities to address information blocking.[70] To this end, the 2015 Edition Certification Proposed Rule[71] includes several measures that would support the certification of health IT that meets relevant program standards and permits the unrestricted use of certified capabilities that facilitate interoperability and electronic health information exchange. These proposed measures include strengthening in-the-field surveillance of certified health IT and requiring more meaningful transparency and disclosure of certain developer practices that may interfere with the performance of technology certified on behalf of ONC.

In response to Congress's request, ONC is also considering under what if any additional circumstances it may be appropriate to terminate certifications issued to health IT under the ONC HIT Certification Program in response to information blocking. Expanding the use of this remedy could be an effective deterrent to certain types of information blocking. However, doing so would be problematic for at least two reasons.

First, terminating a certification may cause widespread and in many cases severe consequences for innocent parties. Under current law, terminating the certification issued to a developer's health IT would not only penalize the developer of that health IT, but also the developer's customers and any other persons who rely on the health IT's certification. In particular, providers who have implemented and are using the health IT, including small provider practices with limited resources, would be unable to demonstrate meaningful use under the EHR Incentive Programs or meet conditions of other federal, state, and private sector programs that incorporate ONC's certification requirements. As a result, they may receive reduced payments under these programs. Moreover, and notwithstanding participation in these programs, providers and other users of the health IT may incur substantial costs to adopt new technologies and services as a result of the termination of the certification for their existing health IT. In addition, contractual and other legal arrangements that also depend on the certification's standing could be affected

Second, expanding the scope of the ONC HIT Certification Program to encompass information blocking would be challenging and require expanding the current approach. To terminate a certification under the current rules, an ONC-ACB must determine that certified health IT no longer conforms to certification criteria,[72] which include specific standards and implementation specifications. Under the existing certification program, requirements aimed at prohibiting information blocking must be tied to compliance with certification criteria for the technology,[73] not the practices of the developer or company that makes the technology or offers the health IT service. This significantly limits the potential reach of such requirements.

As a result of these limitations, terminating a health IT's certification is a blunt instrument that, when applied to bad actors, could cause substantial risk of harm to innocent parties. Moreover, while potentially

---

[70] 160 Cong. Rec. H9047, H9839 (daily ed. Dec. 11, 2014) (explanatory statement submitted by Rep. Rogers, chairman of the House Committee on Appropriations, regarding the Consolidated and Further Continuing Appropriations Act, 2015).
[71] 80 Fed. Reg. 16804 (Mar 30, 2015).
[72] Termination can also be based on the failure of a developer to meet certain program requirements, such as the requirement to disclose certain types of information under 45 C.F.R. § 170.523(k)(1)(iii) and display the ONC Certified HIT Certification and Design Mark as required by 45 C.F.R. § 170.523(l).
[73] *See* Public Health Service Act § 3001(c)(5), 42 U.S.C. § 300jj–11(c)(5).

an effective deterrent to developers from engaging in certain kinds of information blocking, terminating a certification on the basis of many types of information blocking is not currently feasible due to the focus of certification criteria on technical and related requirements. Moreover, this remedy is available only against developers, not providers and other persons or entities who may engage in information blocking. Consequently, to effectively and comprehensively target and deter information blocking, other approaches will also be necessary.

Limitations of Program Oversight for Addressing Information Blocking by Providers

ONC cannot take direct action against providers who block information, and current conditions of participation in federal health care programs do not specifically prohibit information blocking. ONC will coordinate within HHS and with other federal agencies to explore whether creating and enforcing conditions of participation against information blocking would be feasible under these programs. Given the difficult evidentiary challenges and complex questions of fact and interpretation presented, the task of investigating and confirming cases of information blocking may be better suited to an agency or agencies with enforcement expertise and compulsory processes for obtaining evidence.

Inadequate Legal Protections and Enforcement Mechanisms for Information Blocking

Even in egregious cases, most information blocking does not violate any current provision of law. In very specific and limited circumstances, certain types of information blocking may be illegal under one or more federal or state laws, some of which are referenced in this report. But these laws were not enacted to specifically address most information blocking. As a result, investigation and enforcement of information blocking is largely incidental and not responsive in a comprehensive manner to the public policy interests described in this report.

Lack of Transparency and Information about Health IT Products and Services

Requiring developers to be more transparent about business practices that could interfere with the exchange or use of electronic health information would be an effective, market-based approach to preventing many types of information blocking, as described earlier in this section. In particular, providing customers with more reliable and complete information about health IT products and services—and enabling customers to discuss and share this information—would make developers more responsive to customer demands and help ameliorate market distortions that enable developers to engage in certain opportunistic and other behavior that raises serious information blocking concerns.

While ONC is pursuing all avenues to enhance transparency and require more meaningful disclosure of developer business practices that block information, there are limits to the types of information that ONC can require providers and developers to publicly disclose.

First, ONC cannot verify the extent to which developers are using contractual terms to block information (or to conceal information blocking). ONC does not have direct access to developers' contracts with their customers, and customers routinely report that they are prohibited from discussing contract terms due to extremely restrictive non-disclosure and confidentiality provisions in most developers' contracts. On occasion, ONC staff have been exposed to language in developer contracts that prohibits discussion of contract terms—including both price and non-price terms that may be used to restrict information exchange—as well as any *opinions or conclusions* about the performance or any other aspects of the

developer's health IT. In a 2012 report, the Institute of Medicine (IOM) expressed concern that these non-disclosure provisions are chilling discussion of health IT-related safety issues, "which significantly contributes to . . . patient safety risks."[74]

Second, and for related reasons, prospective customers of health IT products and services have very limited visibility into developer pricing practices, which are among the most frequently alleged types of information blocking. Currently, ONC requires developers to disclose, in general terms, certain types of costs associated with specific certified health IT capabilities, but not actual prices or specific price terms.[75] Similarly, while new transparency requirements proposed in the 2015 Edition Certification Criteria Proposed Rule would significantly expand developers' existing disclosure obligations in several important respects, they would not require the disclosure of actual prices or specific price terms. ONC believes that the disclosure of additional, more detailed price information—at least with respect to core interoperability and exchange capabilities—is necessary to ensure meaningful transparency in the health IT marketplace. However, without access to contracts and other evidence, ONC would have difficulty enforcing more detailed price transparency requirements under the ONC HIT Certification Program. Such requirements would also necessitate additional safeguards for the protection of proprietary information, trade secrets, and other sensitive information. In addition, ONC understands that any price transparency requirements would need to avoid potential concerns related to price coordination by competitors.

The persistent lack of transparency and access to reliable information about health IT products and services, including for electronic health information exchange, is a serious problem that not only causes information blocking but substantially impairs the efficient functioning of health IT markets.

Need to Hold Entities Accountable to Governance Principles for Nationwide Health Information Interoperability

As described above and in the draft *Shared Nationwide Interoperability Roadmap*,[76] ONC intends to specify a nationwide governance framework that will establish principles regarding business, technical, and organizational practices related to interoperability and electronic health information exchange. Adherence to these principles would mitigate many types of information blocking, but may require additional authorities to hold entities accountable.

ONC is examining available approaches for establishing an appropriate and effective governance mechanism for nationwide electronic health information exchange. As part of this process, ONC will keep Congress informed about available approaches and any additional authorities that may be needed.

[74] Institute of Medicine (IOM), *Health IT and Patient Safety: Building Safer Systems for Better Care*, 3, 37 (2012) (concluding that non-disclosure clauses in EHR vendor contracts "limit transparency, which significantly contributes to . . . patient safety risks.")
[75] 77 Fed. Reg. 54273–75.
[76] *Roadmap*, *supra* n.11.

CONCLUSION

The intent of the HITECH Act was to drive the rapid adoption of interoperable technologies and services to support the exchange of electronic health information to improve care and efficiency in the U.S. health care system. While this intent was and is clear to most stakeholders, based on ONC's experience and available evidence, the developing market for health IT products and services has, in some instances, fallen short of this charge.

The precise nature and extent of information blocking remain obscured in large part by contractual restrictions that prevent the disclosure of relevant evidence. However, based on the evidence and knowledge available, it is apparent that some health care providers and health IT developers are knowingly interfering with the exchange or use of electronic health information in ways that limit its availability and use to improve health and health care. This conduct may be economically rational for some actors in light of current market realities, but it presents a serious obstacle to achieving the goals of the HITECH Act and of health care reform.

There are several immediate actions ONC, HHS, and other federal agencies can take to partially address some kinds of information blocking. In this report, ONC has outlined a number of targeted actions to deter and mitigate such conduct, within limited areas.

While important, these actions alone will not provide a complete solution to the information blocking problem. Indeed, a key finding of this report is that many types of information blocking are beyond the reach of current federal law and programs to address. Thus a comprehensive approach will require overcoming significant gaps in current knowledge, programs, and authorities that limit the ability of ONC and other federal agencies to effectively target, deter, and remedy this conduct, even though it violates public policy and frustrates congressional intent. For these reasons, in addition to the actions outlined in this report, successful strategies to prevent information blocking will likely require congressional intervention.

Information blocking is certainly not the only impediment to an interoperable learning health system. But the findings in this report suggest that it is a serious problem—and one that is not being effectively addressed. ONC believes that in addition to the actions described in this report, there are several additional avenues open to Congress to address information blocking and drive continued progress towards the nation's health IT and health care goals. ONC looks forward to working with Congress to identify the best solutions.

APPENDIX A — INFORMATION BLOCKING SCENARIOS

Identifying and confirming specific instances of information blocking is a difficult and highly fact-specific task. The following hypothetical scenarios illustrate how the criteria and other considerations described in this report can be applied in real-world situations. These scenarios draw from common allegations and themes reported in actual complaints and anecdotes of information blocking. However, the facts of each scenario are strictly hypothetical and are not intended to implicate any particular person or entity.

Scenario #1: Refusing to Share Core Clinical Information with a Rival ACO

Two competing health care provider organizations ("Blocking ACO" and "Competing ACO") have adopted ONC-certified health IT and received payments under Stage 2 of the EHR Incentive Programs. Both ACOs are capable of safely, securely, and effectively sending and receiving patients' basic clinical information electronically for treatment or other authorized purposes, and no applicable federal or state privacy law prohibits this practice. However, Blocking ACO will only send health information about Competing ACO's patients via fax. Blocking ACO knows that faxing patient records (which are often hundreds of pages long) is more expensive and less efficient than sending them electronically. In particular, data must be manually entered by the recipient—an expensive and time-consuming process that can be automated and made more reliable by exchanging and incorporating the information electronically.

Analysis: Blocking ACO is likely engaging in information blocking.

Blocking ACO's express policy to send information by fax and not electronically interferes with Competing ACO's timely access to reliable electronic health information. And as an ACO whose physicians have achieved Stage 2 of the EHR Incentive Programs, Blocking ACO should know that its actions will cause that result.

Blocking ACO's conduct also appears to be unreasonable because the refusal to electronically send basic clinical information for patient care raises serious information blocking concerns[77] and lacks any reasonable justification under these facts. The refusal not only interferes with health information exchange but also undermines patient safety by reducing the timeliness and reliability of clinical information about Competing ACO's patients. Moreover, the interference appears to be avoidable. The facts state that Blocking ACO is capable of safely, securely, and effectively sending this information and at less cost than faxing it. There is also no apparent privacy or security justification for refusing to share this information electronically.[78]

Blocking ACO might argue that its actions are justified because electronically sharing this information with its competitors is not in Blocking ACO's economic self-interest. Blocking ACO might also assert that by competing vigorously with other ACOs it is advancing the broader interests of competition and consumers. While it is probably true that Blocking ACO's actions advance its own competitive position,

[77] For the reasons provided in section II of this report, "[p]ractices that knowingly interfere with health information exchange are especially problematic when they . . . restrict providers and other authorized persons from *exchanging basic clinical information necessary for effective patient care*." *Supra* pp. 12–13 (emphasis added).
[78] The disclosed faxed records are a form of exchange (albeit one that is expensive, old fashioned, unsecure, and error-prone due to reentry).

they do so not because they enable Blocking ACO to deliver better or more efficient care (in fact, faxing information costs more and is more time-consuming for staff) but by reducing the quality and efficiency of care that its competitors can provide (by denying them access to basic clinical information about their patients). But this harms, not benefits, consumers. Overall, Blocking ACO's proffered economic arguments are marginal and do not outweigh the public policy concerns raised above.

Scenario #2: Service Provider Security Concerns

Service Provider operates services and infrastructure that facilitate health information exchange for health care providers across the country that participate in a known trust community where security and business practices are verified and members of the trust community are held accountable to agreed-upon security and business best practices. However, Service Provider does not allow connections to other health information exchange service providers that do not participate in this trust community. By refusing to connect with service providers that are not part of the trust community, Service Provider limits the data trading partners with whom their customers can electronically exchange health information. That is, Service Provider's customers can only electronically exchange health information with data trading partners who use services provided by other members of the trust community.

Analysis: It is unclear whether this scenario reflects information blocking.

Service Provider is knowingly interfering with the ability of its customers to electronically exchange health information with persons or entities that are not members of its trust community. However, without additional facts, it is unclear whether this interference is unreasonable. There may be specific circumstances and experiences that warrant the limitation of information exchange only with organizations/service providers that adhere to the same "best practices" in security. It may also be true that adherence to "best practices" is not *legally* warranted and may be more of a business practice than a compliance or liability-reducing mechanism. (This scenario does not include any analysis of whether information exchange by the provider using Service Provider was requested by or at the direction of an individual or patient.)

Scenario #3: "Kill Switch"

Provider licenses EHR software from Vendor. The software is installed on Provider's computer systems but maintained by Vendor, a business associate of Provider under the HIPAA Rules. Provider and Vendor are involved in a billing dispute. Provider disputes and refuses to pay certain service charges. Vendor files suit for breach of contract and simultaneously notifies Provider of its intention to terminate Provider's access to Vendor's software unless the outstanding balance is paid in full within 30 days. When Provider does not pay, Vendor activates a "kill switch" that it embedded in its software during a routine software update. The kill switch, once activated, encrypts all patient health records stored on Provider's computer systems and renders the data inaccessible to Provider and its patients.

Provider demands that Vendor restore access to the health records until the lawsuit is resolved. When Vendor refuses, Provider requests temporary access for 48 hours so that it can retrieve its patients' records. Vendor refuses even though it could grant Provider's request without incurring any significant costs. Provider ultimately obtains an injunction compelling the release of its records, but in the meantime Provider's clinicians are unable to access basic clinical information necessary for patient care (e.g., diagnoses, medications, and test results).

Analysis: On these facts, Vendor has engaged in information blocking.

By embedding and then activating a "kill switch" in its software, Vendor interfered with Provider's access to its patients' health information. Vendor also knew that its actions would have this result because it designed, embedded, and activated the "kill switch."

Vendor's actions were unreasonable for several reasons. They were likely—in fact, certain—to interfere with Provider's access to clinical information necessary for patient care. Such conduct raises serious public policy concerns[79] that, absent a reasonable justification, result in information blocking. On these facts, no reasonable justification exists: Vendor's conduct was not necessary to protect patient safety, maintain the privacy or security of health information, comply with applicable law or legal duty, or advance any other countervailing interest. With respect to Vendor's legitimate economic interests, Vendor cannot plausibly make a financial hardship argument because the facts clearly state that Vendor could have granted Provider access for 48 hours without incurring any significant costs. Vendor also had and was pursuing a remedy under state law for its alleged financial damages.

Vendor's attempt to use control over individuals' electronic health information as leverage in a contract dispute further supports the conclusion that its actions were unreasonable and therefore constituted information blocking.

Finally, vendor's refusal to make available electronic PHI to the health care provider may be a violation of state and/or federal security laws that require the *availability* of patient health information be maintained.

Scenario #4: Information Blocking to Lock in Referrals

A small provider ("Provider") frequently orders tests from a local lab operated by a national laboratory chain ("First Lab"). First Lab operates a separate line of business as a developer of EHR technology certified by ONC. By licensing its EHR technology to physicians and making it easy to exchange orders and results electronically with its local lab, First Lab is able to encourage referrals to its local lab.

Provider has adopted First Lab's EHR technology and is using it to electronically order and record lab results as required for Stage 2 of the EHR Incentive Programs. During the Stage 2 reporting period, a major commercial health plan ("Plan"), the largest in Provider's community, switches its preferred lab to First Lab's main competitor ("Second Lab"). Provider requests to purchase at full cost an interface from First Lab to connect its EHR technology to Second Lab's electronic ordering system so that Provider can continue to order and receive lab results for all patients. Because it competes with Second Lab in the market for lab services, First Lab has a blanket policy not to enable interfaces from its EHR technology to any Second Lab labs. First Lab could technically establish such interfaces and in fact routinely builds interfaces to many other ancillary health IT systems. First Lab also builds such interfaces to competing labs, provided they are not operated by Second Lab.

As a result of First Lab's refusal to establish an interface to Second Lab's lab, Provider is unable to electronically order and record lab results for most of its patients and is also unable to meet the Stage 2 requirements for an incentive payment.

Analysis: On these facts, First Lab is engaging in information blocking.

[79] *See supra* n.77.

First Lab's refusal to build a lab interface interferes with Provider's ability to exchange basic clinical information (lab orders and results) for patient care. First Lab knows its conduct will (and, on these facts, intends to) prevent Provider from exchanging information with Second Lab's lab.

For the following reasons, First Lab's refusal to establish interfaces to Second Lab's labs is unreasonable and amounts to information blocking.

First Lab's refusal interferes with the exchange of clinical information for patient care. It therefore raises serious information blocking concerns for the public policy reasons described in section II of this report. As such, a compelling justification must exist for the interference with health information exchange to be reasonable and not information blocking.

No such justification exists on the facts of this scenario. There are no evident privacy or security justifications for the refusal to establish interfaces with Second Lab's labs, and the fact that First Lab successfully interfaces with a wide range of other health IT systems—including other competing lab systems—suggests that the refusal is not necessary to ensure a reliable, safe, or superior lab ordering experience. For the same reasons, any suggestion that the refusal is necessary to protect patient safety is also implausible, as is the suggestion that the refusal results in any significant economic benefits to First Lab's customers in the form of a superior product or service.

Instead, First Lab's refusal evinces a business strategy to use its EHR technology to control referrals in the separate market for lab services and, in doing so, prevent customers from doing business with its main competitor in that market. This strategy may be economically rational for First Lab, but for the reasons above, offers no substantial benefit to First Lab's customers, patients, or consumers at large. Meanwhile, the refusal to establish interfaces solely on this basis has substantial repercussions for Provider and other similarly situated customers, who are unable to meet the requirements of the EHR Incentive Programs and, more importantly, are prevented from delivering safer and more effective care to their patients.

Against these indications, First Lab's knowing interference with the exchange of electronic health information is not necessary to advance any important interest so compelling that it outweighs the strong public policy in favor of promoting access to such information, especially basic clinical information, for authorized purposes. Because it has no reasonable justification, First Lab's conduct is information blocking.

Scenario #5: Overbroad Privacy Policy

Hospital A operates certified EHR technology in State A. State A has a state health information privacy law that expressly permits hospitals that are licensed to provide inpatient mental health treatment to disclose information related to that treatment to other health care providers for treatment without consent. In addition, the HIPAA Rules permit covered entities to disclose PHI to health care providers for treatment purposes without consent, regardless of locale. No heightened privacy or security risks have been identified related to treatment disclosures across state lines.

Sue, who has received inpatient mental health treatment in Hospital A in the past, has been admitted to Hospital B for mental health treatment. Hospital B has a mental health wing and operates certified EHR technology in the neighboring State B. State B has a general health information privacy law that incorporates HIPAA by reference; another state law specifically requires hospitals to obtain patient consent before releasing information related to mental health inpatient treatment.

Hospital B obtains Sue's consent and requests her electronic health record from Hospital A. Hospital A, though technically capable of sending Sue's record, has an internal privacy policy not to share mental

health information with out-of-state providers. Hospital A knows that no laws prevent it from sending Sue's electronic health information to Hospital B, and knows that Sue consented to Hospital B asking for her record. Yet Hospital A still refuses to send the information, stating it cannot due to "privacy" laws. On the basis of this policy, Hospital A does not share Sue's electronic health information with Hospital B.

Analysis: Hospital A's conduct may constitute information blocking.

Hospital A is interfering with the exchange of electronic health information because of its internal policy not to share mental health information with out-of-state health care providers. Hospital A sharing the information with Hospital B (making the disclosure) for treatment purposes is consistent with both state and federal law. Hospital A has knowledge that its conduct will interfere with exchange. Hospital A does not appear to have a reasonable justification in applying an internal privacy policy structured around the location of the other treating health care provider, because no apparent increased privacy risk nor privacy law requirements would stand in the way of making these disclosures for treatment purposes.

APPENDIX B — ONC HIT CERTIFICATION PROGRAM

Section 3001(c)(5) of the Public Health Service Act (PHSA) provides the National Coordinator with the authority to establish a certification program or programs for the voluntary certification of health information technology. Specifically, this section requires the National Coordinator, in consultation with the Director of the National Institute of Standards and Technology (NIST), to keep or recognize a program or programs for the voluntary certification of health information technology as being in compliance with certification criteria adopted by the Secretary. Section 3001(c)(5) also requires that the ONC administered certification program(s) must include, as appropriate, testing in accordance with section 13201(b) of the HITECH Act, which requires that with respect to the development of standards and implementation specifications, the Director of NIST support the establishment of a conformance testing infrastructure, including the development of technical test beds.

In developing the ONC HIT Certification Program, ONC consulted with NIST and created its certification program based on industry best practice. This structure includes the use of two separate accreditation bodies. An accreditor that evaluates the competency of a health IT testing laboratory to operate a testing program in accordance with international standards and, similarly, an accreditor that evaluates the competency of a health IT certification body to operate a certification program in accordance with international standards. After a certification body is accredited, it may apply to the National Coordinator to receive authorization to certify health IT ONC's behalf. Once authorized, these certification bodies are referred to as ONC-Authorized Certification Bodies or ONC-ACBs. The ONC HIT Certification Program includes a full process by which ONC oversees the operations of ONC-ACBs and includes the potential issuance of certain types of violations as well as a process to revoke an ONC-ACBs authorization to certify on ONC's behalf.

With respect to ONC-ACBs and the international standard to which they are accredited, they are uniquely positioned and accountable for determining whether a certified product continues to conform to the certification requirements to which the product was certified. If an ONC-ACB can substantiate a non-conformity, either as a result of surveillance or otherwise, the international standard requires that the ONC-ACB consider and decide upon the appropriate action, which could include: (1) the continuation of the certification under specified conditions (e.g. increased surveillance); (2) a reduction in the scope of certification to remove nonconforming product variants; (3) suspension of the certification pending remedial action by the developer; and (4) withdrawal/termination of the certification.