# Information Blocking Task Force Recommendations

May 22, 2019

May 22, 2019
Carolyn Petersen, co-chair
Robert Wah, co-chair
Health Information Technology Advisory Committee
Office of the National Coordinator for Health Information Technology
Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

Dear Carolyn and Robert,

The Health Information Technology Advisory Committee (HITAC) requested that the Information Blocking Task Force (IBTF) provide recommendations to the HITAC regarding the proposals in the Cures Act Notice of Proposed Rulemaking related to information blocking. This transmittal letter offers those recommendations, which the IBTF wishes to advance to the HITAC for consideration. These recommendations are informed by extensive deliberations among the IBTF subject matter experts.

We believe that there are several aspects of these recommendations which warrant additional exploration to ascertain the impact upon different stakeholder groups, and to provide guidance to them. This is not a suggestion to defer any recommendations, but to provide additional clarity to those stakeholder groups and to assist in the adoption of the 21st Century Cures Act and ensuring the benefits thereof. It is our profound belief that HITAC is best positioned as the agent to assist in this regard.

As co-chairs of the IBTF, we wish to thank the HITAC for the opportunity to serve in this fundamental role supporting the success of ONC's Proposed Rule and the rulemaking process and promoting improved patient outcomes through information sharing. The discussions of the IBTF have been exhaustive, in no small part due to the diligence and expertise demonstrated by the ONC staff assigned to support this task force. We thank them for their contributions.

Please consider the attached recommendations from the IBTF. Each recommendation is individually numbered, and where recommendations have been removed compared to prior late-stage drafts, we have preserved the original numbering to promote appropriate version control.

Yours faithfully,

Michael Adcock
Andy Truscott

**Table of Contents**

## Background

### Overarching charge

The Information Blocking Task Force (IBTF or Task Force) was charged with providing recommendations on proposals in the Cures Act Notice of Proposed Rulemaking (ONC's Proposed Rule or Proposed Rule) related to information blocking; the "information blocking," "assurances," and "communications" conditions and maintenance of certification requirements; and the enforcement of all the conditions and maintenance of certification requirements.

### Detailed charge

The IBTF was charged with providing recommendations on the following topics:

- Information Blocking:
  - ONC proposed definitions/interpretations of certain statutory terms and provisions, including the price information request for information
  - Seven proposed exceptions to the information blocking definition, and any additional exceptions (request for information)
  - Complaint process
  - Disincentives for health care providers (request for information);
- "Information blocking," "assurances," and "communications" conditions and maintenance of certification requirements; and
- Enforcement of all the conditions and maintenance of certification requirements.

### Task Force Approach

In addressing the IBTF's charge, the co-chairs separated the subject matter into three distinct workgroups.

1. The first workgroup considered ONC's proposed definitions and interpretations of certain statutory terms and provisions, including the price information request for information.

2. The second workgroup considered the seven proposed exceptions to the information blocking definition; any additional exceptions (request for information); the complaint process; and disincentives for health care providers (request for information).

3. The third workgroup considered the "information blocking," "assurances," and "communications" conditions and maintenance of certification requirements; and enforcement of all the conditions and maintenance of certification requirements.

During the workgroup deliberations, the co-chairs provided a level of autonomy to each workgroup in order to promote focused review and manage workloads. Once the co-chairs drafted and refined recommendations for each workgroup, the IBTF met multiple times as a whole and together reviewed and finessed our recommendations into the form detailed below.

## ONC Definitions/Interpretations of Certain Statutory Terms and Provisions

ONC's definitions and interpretations of statutory terms and provisions provide the bedrock for ONC's information blocking proposals and the scope of actors and actions to be covered by the information blocking provision. The IBTF spent considerable time evaluating, weighing, and measuring the regulatory text as drafted, and has made thoughtful proposals based upon the members' experiences and input.

### 1. Health Information Network / Health Information Exchange

We recognize that there are multiple uses of the terms "Health Information Network" (HIN) and "Health Information Exchange" (HIE) across the healthcare ecosystem. Having the terms overlap within the Proposed Rule is likely to cause a degree of confusion. We believe that defining HIE as a process, which can be undertaken by a HIN or a provider using software and/or services created by a HIT developer, should provide a level of clarity. Removing the word "exchange" from the definition of "Health information Exchange" should provide further clarity.

This recommendation is supported by the language of 21st Century Cures that considers:

> "...entering into agreements with health information exchange networks may require…" (section 4003(b)(9)(E)), which the IBTF believes makes clear that there exists networks of organizations or individuals performing health information exchange.
>
> "... (c) Promoting Patient Access to Electronic Health Information Through Health Information Exchanges…encourage partnerships between health information exchange organizations and networks and health care providers, health plans, and other appropriate entities…" (section 4006(c)(1)), which could be read in the title as an 'exchange' being either the promotion of patient access using an 'HIE organization' for exchange, or the promotion of patients access through exchanges of health information. The subsequent legislative text talks about 'health information exchange

organizations' which seems to support the position of an organization who conducts the act of exchanging health information.

However, there is contrasting reference to:

> "...by public and private organizations related to exchange between health information exchanges.." (section 4003(b)(9)(F)), where exchange can take place between such 'health information exchanges'.
>
> "a health information exchange or network engaged in information blocking" (section 3022(b)(1)(C)), where there is consideration of both an 'exchange' or 'network'.

To this end, for information blocking purposes, we consider those organizations or individuals who consider themselves to be an organization or individual of the type "Health Information Exchange" to be a "Health Information Network" that conducts the act of "Health Information Exchange".

In section 4006 of the 21st Century Cures Act (Cures Act) there is an additional potential definition – "health information exchanges (or other relevant platforms)"– that could be read as indicating that 'health information exchange' is a technology type, or that it is a technology that supports the act of exchanging health information. However, later in section 4006 there is a reference to "...shall issue guidance to health information exchanges related to best practices…" This appears to be a clear indication that a 'health information exchange' should be considered an entity unto whom guidance can be issued.

## Recommendations 1 (HIE definition) & 2 (HIN definition)

| **§ 171.102 Definitions of Health Information Exchange and Network** | | |
|---|---|---|
| ORIGINAL | RECOMMENDED REGULATION TEXT | COMPARISON / MARKUP |
| *Health Information Exchange or HIE* means an individual or entity that enables access, exchange, or use of electronic health information primarily between or among a particular class of individuals or entities or for a limited set of purposes.<br><br>*Health Information Network or HIN* means an individual or entity that satisfies one or both of the following—<br>(1) Determines, oversees, administers, controls, or substantially influences policies or | *Health Information Exchange* or *HIE* means:<br><br>Any entity performing the access, exchange, transmittal, processing, handling, or other such use of Electronic Health Information who is not considered a Provider, Health Information Network, or Health IT Developer.<br><br>*Health Information Network* or *HIN* means an individual or entity that satisfies one or several of the following— | *Health Information Exchange or HIE* means:<br><br>~~a~~Any ~~individual or~~ entity performing the ~~that enables~~ access, exchange, transmittal, processing, handling or other such use of ~~e~~Electronic ~~h~~Health ~~i~~Information ~~primarily between or among a particular class of individuals or entities or for a limited set of purposes.~~ who is not considered a Provider, Health Information Network, or Health IT Developer. |

| | | |
|---|---|---|
| agreements that define business, operational, technical, or other conditions or requirements for enabling or facilitating access, exchange, or use of electronic health information between or among two or more unaffiliated individuals or entities.<br>(2) Provides, manages, controls, or substantially influences any technology or service that enables or facilitates the access, exchange, or use of electronic health information between or among two or more unaffiliated individuals or entities. | (1) Determines, oversees, administers, controls, or sets policies or makes agreements that define business, operational, technical, or other conditions or requirements for Health Information Exchange between or among two or more individuals or entities, or<br><br>(2) Provides, manages, or controls any technology or service that enables or facilitates Health Information Exchange between or among two or more individuals or entities. | *Health Information Network or HIN* means an individual or entity that satisfies one or ~~both~~ several of the following—<br><br>(1) Determines, oversees, administers, controls, or sets ~~substantially influences~~ policies or makes agreements that define business, operational, technical, or other conditions or requirements for Health Information Exchange ~~enabling or facilitating access, exchange, or use of electronic health information~~ between or among two or more ~~unaffiliated~~ individuals or entities.<br><br>(2) Provides, manages, or controls ~~or substantially influences~~ any technology or service that enables or facilitates Health Information Exchange ~~the access, exchange, or use of electronic health information~~ between or among two or more ~~unaffiliated~~ individuals or entities. |

*Explanation of Recommendation*

We recognize that there is ambiguity with the use of "Health Information Exchange" and "Health Information Network" within the healthcare industry. We are defining and using the terms not interchangeably, but with a clear distinction between the act of performing the exchange of electronic health information, and the organization or individual who performs that act.

*Potential Alternative Approach*

A potential alternative approach to the distinction between HIE and HIN could be to eliminate the distinction completely, and simply define HIE and HIN as meaning the same by using the above definition of HIN and referencing both HIE and HIN as having that meaning.

## 2. Electronic Health Information (EHI)

The IBTF believes the proposed definition of "electronic health information" (EHI) is a strong definition that covers the breadth of data that should be addressed within the regulation. We recommend some slight modifications to the language to cover both current and future tenses

(can vs could) and to address where discrete data may not identify an individual, however, in aggregate it may.

Our intent is that this is a broad definition that embodies a wide range of information concerning patient care. Furthermore, "information" shall be inclusive of all data that can be electronically transmitted or maintained and may include imaging.

Discussion has also looked at whether, in the Cures Act, Congress was seeking to aid transparency across the healthcare ecosystem and whether the definition should be limited to identifiable health information or whether it should include all information within healthcare.

Our recommendation around the sharing of consent information aligns with the anticipated ratification dates for the HL7 FHIR standard for communication of these information types, and the IBTF believes that including consent information is extremely important to meet the intent of the Cures Act.

An additional minor update would be to clarify that we are not seeking to promote the sharing of information for a specific payment (use of the singular "payment"), we are desiring that information for all payments should be covered within this definition. To this end, we recommend pluralizing "payment."

In addition, we do think that making clear that "information" could be that which is "human readable" (e.g., narrative text captured within clinical notes) and "machine readable" (e.g., codified information using terminologies or classifications such as LOINC, SNOMED CT, CPT, ICD etc.) are specifically covered to prevent ambiguity, and this should be updated within the preamble.

Recommendation 3

| § 171.102 Definition of Electronic Health Information | | |
|---|---|---|
| ORIGINAL | RECOMMENDED REGULATION | COMPARISON / MARKUP |
| *Electronic Health Information (EHI)* means—<br>(1) Electronic protected health information; and<br>(2) Any other information that identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual and is transmitted by or maintained in electronic media, as defined in 45 CFR 160.103, that relates to the past, present, or | *Electronic Health Information (EHI)* means—<br>(1) Electronic protected health information (as defined in 45 CFR 160.103); and<br>(2) Electronic Individual Health Information:<br>(i) Any other information that identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual and is transmitted by | *Electronic Health Information (EHI)* means—<br>(1) Electronic protected health information (as defined in 45 CFR 160.103); and<br>(2) Electronic Individual Health Information:<br>(i) Any other information that identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual and is transmitted by |

| | | |
|---|---|---|
| future health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. | or maintained in electronic media, as defined in 45 CFR 160.103, that relates to the past, present, or future health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment(s) for the provision of health care to an individual.<br>(ii) On the two-year anniversary of the effective date of the final rule, an individual's consent directives including privacy, medical treatment, research, and advanced care.<br>(3) Electronic information which can reasonably be used to inform care decisions, by a provider or patient, including pricing information which can be attributable to an individual patient. | or maintained in electronic media, as defined in 45 CFR 160.103, that relates to the past, present, or future health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment(s) for the provision of health care to an individual.<br>(ii) On the two-year anniversary of the effective date of the final rule, an individual's consent directives including privacy, medical treatment, research, and advanced care.<br>(3) Electronic information which can reasonably be used to inform care decisions, by a provider or patient, including pricing information which can be attributable to an individual patient. |

Recommendation 4

Within the definition of Electronic Health Information, the term "information" shall be read as applying to both "Human Readable" information that can be readily understood by a real person actor without specialized reference (e.g., narrative clinical notes), and also "Machine Readable" information that is interpreted by a computerized actor for use either by computerized processes or a real person actor (e.g., data codified using a terminology or classification).

Minority Opinion**:** Concern has been expressed by a minority of the IBTF that the definition of EHI is overly restrictive in that it demands that information should identify an individual. This minority opinion suggests that ONC should adopt a revised definition of EHI in the final rule that would remove the requirement that the information be identifiable. The minority opinion believes this change will ensure that information blocking supports patient access to price information to enable shopping for health care services. ONC should also clarify that "future payment" includes price information.

The minority opinion believes that the proposed ONC definition is inconsistent with congressional intent of the Cures Act and definitions in existing law since 1996 (HIPAA). The Cures Act prohibits information blocking of EHI and this term is not defined in the Cures Act. As such, the minority opinion contends that ONC should look to prior definitions in defining this term to effectuate the intent of Congress.

The minority opinion believes that the simplest and most logical interpretation of "electronic health information" is to use the definition of "health information" which is not limited to identifiable information. The minority opinion believes that Congress knew there were different terms for "health information", "individually identified health information", and "protected health information" under HIPAA when it drafted the Cures Act and wished to include all of these within the Cures Act. Congress did not use the term Electronic Individually Identifiable Health Information, which would have limited information blocking to identifiable information.

## 3. Price Information Request for Comment and Request for Information

Recommendation 5

The IBTF profoundly agrees that price transparency is a desirable goal that is achievable. We further believe that policy levers are required to move the healthcare ecosystem in that direction given the nature of reimbursement. We believe that tying the information blocking proposals in the Proposed Rule too tightly with potential proposals that would be necessary to promote price transparency may have the unintended consequence of slowing down the finalization of the current ONC rule. The finalization of the current rule (an already daunting task) could be delayed while language to address price transparency is being considered and drafted.

The IBTF notes that the proposed definition (along with our recommendations for amendment) provide for an expansive set of EHI, which could include information on an individual's health insurance eligibility and benefits, billing for health care services, and payment information for services to be provided or already provided, which may include price information, and that this intent should be preserved.

The IBTF notes that availability of individually specific price information enables patient to shop for and make informed decisions about their care, and that it should be included in the scope of EHI as per our recommendations.

The IBTF notes that existing entities within the healthcare ecosystem have access to pricing information which could be utilized by patients to make informed decisions about the nature and location of their care. Those entities should be obliged to share that information, and our recommended amendment to the definition of EHI is designed to promote the sharing of that information by placing non-sharing within the boundary of information blocking.

The definition of EHI encapsulated within the Proposed Rule includes clear reference to "...or the past, present, or future payment(s) for the provision of health care to an individual." This ensures that the right information is being exchanged and the IBTF believes that regulations that address price transparency could be built upon this solid interactive base.

To this end, we recommend that ONC instantiates through HITAC a task force specifically charged with producing recommendations for future rulemaking to address improving price transparency across the healthcare ecosystem.

This newly instantiated task force should consider:

- How generalized price information can be made readily accessible and available to patients, providers, purchasers, payers and other relevant stakeholders to inform care decisions.

- That the coding for prices can be published simply by using the rate cards between the providers and the payers.

- Whether to get to price transparency, patients need to know the contract negotiated rates.

- How those involved in the financial transactions to support healthcare delivery should provide the real prices. By CPT code or DRGs, bundled and unbundled?

- Whether prices included in the definition of EHI should reflect all services and payment information by all parties (including, but not limited to, health care providers, health plans, insurers, contractors, administrators, pharmacy benefit managers (PBMs), pharmacies, group purchasing organizations (GPOs), technology companies, health IT developers, laboratories, medical devices, brokers and other similar market players).

- The manner in which contract terms, rebates or other forms of incentive payment or other form of remuneration that is or will be directly attributable to a specific service, patient charge or transaction, to a health care provider, facility, pharmacy, or medical equipment provider for the health care services, drugs, or equipment delivered is logged and communicated.

## 4. Health IT Developer of Certified Health IT

The IBTF believes clarity is required concerning health IT developers who have at least one product certified under the ONC Health IT Certification Program (Program) and those developers of health IT that do not seek certification under the Program. We believe the number of developers that fall into the latter category will be ever-increasing over the coming years, for several reasons. New entrants to the health IT market that provide niche services to patients may not seek certification, especially if they are consumer focused instead of clinical. New and existing entrants may not seek certification as they adopt alternative business

models which reduce the cost of health IT to end users, and therefore have reduced incentive for certification.

The IBTF wishes to promote innovation and prevent barriers for entry for products that may have important benefits to patients. The IBTF is also mindful that by limiting the applicability of the regulation to only developers of certified health IT there might be the unintended consequence of encouraging developers to not comply with the regulation, which could encourage information blocking practices amongst those non-regulated vendors.

This, coupled with a movement towards self-developers and operators of healthcare-related services could create a "second track" of non-compliant actors being detrimental to the integrated patient care and transparency we desire to foster and promote.

In addition, the IBTF notes that the two following conditions appear to be in error and at odds with the intent of the Cures Act:

- The position that a product developed is "covered" if it is certified, or if the developer also produces a product that is certified, seems not in keeping with the perceived Congressional intent of the Cures Act that if a product is handling EHI then the developer should be covered by the information blocking provision; and

- Depending on what ONC finalizes within the rule process a developer of health IT who may have their products certified, and have that certification terminated or suspended for whatever reason, could potentially find that the regulations no longer apply to them.

Recommendation 6

We recommend clarifying that a developer of health IT is a developer because they create IT designed to perform the access, exchange, or use of EHI whether or not that IT is certified.

The IBTF recognizes that the Cures Act does not provide the necessary statutory powers to promote sanctions against health IT developers who are not producing certified health IT, and that while this may be an enforcement gap, it does not mean that some developers should not be subject to the information blocking provision.

## 5. Practices That May Implicate the Information Blocking Provision

**Actors vs. Information Type**

The IBTF believes that the information blocking provision is designed to ensure that patient information moves without hindrance across the healthcare ecosystem with appropriate authorization to facilitate the provision and reimbursement of care services to patients. These

services are likely to be provided by an increasingly broad series of organizations, and these regulations must be structured so that these new entrants to the market are appropriately covered by the conditions herein. It would not be advantageous to improving patient outcomes if some actors were implicated (through inclusion) and others were not (by the regulations being mute) as the regulations should consider the blocking of information versus the entity performing the blocking.

Recommendation 7

[This recommendation has been removed]

**Pricing Information**

The Task Force believes that pricing information is an area that could readily implicate the information blocking provision. This information is not routinely exchanged and will require focus from multiple actors to ensure that the intent of Congress is met. This issue is addressed in more detail in an earlier recommendation.

Recommendation 8

*Patient Access* - The Task Force believes that "open" patient access to EHI about them is likely to have implications that relate to the information blocking provision. The obligation of actors to provide such access in real-time, and free of charge (beyond approved fee exemptions) is not one that is widely understood or implemented now (even in a "paid" manner). Similarly, providing patients with the tools to appropriately parse EHI to ensure it is understandable to them may potentially have implications that relate to the information blocking provision and ONC should investigate whether this is the case.

## 6. Parties Affected by the Information Blocking Provision and Exceptions

The Task Force believes that there is opportunity for confusion as to the parties implicated by the information blocking provision and exceptions, and ONC should take steps to remediate this in the final rule.

The Task Force believes that one intention of the Cures Act is for parties who are accessing, exchanging, or otherwise using information about a patient to provide patient care to be implicated by the regulations. The definitions of "actors" within the Cures Act do not have clear boundaries so that organizations can understand whether they are one of the four "actors" defined (provider, health information network, health information exchange, or health information technology developer) to understand whether they are implicated by the information blocking provision.

Recommendation 9

[This recommendation has been removed]

Recommendation 10

The IBTF recommends that the preamble be updated to give greater specificity as to the real-world organizational types who could fall into the various categories of Actors. For example:

- Retail pharmacies who curate patient information concerning prescriptions, medications, clinical histories, payments etc. This information is considered EHI and should not be blocked. The IBTF believes that Retail Pharmacy would already be considered a Provider through inclusion as a subpart of all Pharmacies. This is desirable to confirm.

- Insurance companies who curate patient information concerning medical histories, payments etc. This information is important to patients as they seek to obtain insurance coverage for care services.

- Retailers who provide patient information services through IoT type devices and services from connected consumer devices. This information is considered EHI and must not be blocked.

We recognize that with the healthcare environment being under constant change, parties may act as one or more than one of the "actor" definitions, and the regulations should recognize that.

Recommendation 11

The IBTF recommends that the preamble should also be updated to give greater specificity as to the real-world organizational types who **would not** fall into these categories and **would not** therefore implicate the information blocking provision. For example:

- Organizations to whom patients have expressed informed **dissent** for information sharing (and this should remain an exception to information blocking under the privacy sub-exception for *respecting an individual's request not to share information*);

- Social media networks who provide access to non-specific patient attributable health information, and

- Analytics companies who provide population health insights based upon non-specific patient data (although a company who provides insights which may be used specific to an identifiable individual **would** implicate the information blocking provision).

The IBTF also recognizes that there are other individual entities who a patient may wish to have access to information about that patient, such as care givers, proxies, etc.

Recommendation 12

The TF recommends adopting a position of inclusion for implication based upon an actor's access, exchange, or use of EHI as well as their role in the healthcare ecosystem. We recommend specifically identifying that an entity should not share EHI where a patient has expressly stated their information should not be shared (and this should remain an exception to information blocking under the privacy sub-exception for *respecting an individual's request not to share information*).

Recommendation 13

The TF recommends adding the following text to the preamble and ensuring alignment of existing text to it:

The healthcare environment is under constant change. A tight definition of the term "Actor" may only be valid on the day it is authored and for a short time afterwards. By focusing the definition of a relevant "Actor" upon the function they undertake and including covered actors through their actions as opposed to their inclusion within a group we seek to afford evolutionary coverage through this regulation.

## Exceptions

The IBTF has spent considerable time considering the exceptions to the information blocking provision, and the precise meaning of the verbiage expressed. Our recommendations reflect an overwhelming desire to promote clarity and simplicity in the final rule as far as possible, while reflecting the intent of Congress in the Cures Act.

## 7. Preventing Harm

The IBTF applauds ONC for including the provision "Exception – Preventing Harm" in the Proposed Rule. Actors engaged in the access, exchange, and use of EHI must be assured that practices that prevent harm are not an unintended consequence of promoting interoperability. We discussed that the recurring theme of having consistent and non-discriminatory policies are critical as this exception should be rarely applied and when applied should not be a mechanism to selectively block information from specific actors. We also discussed the importance of the inclusion of an exception to prevent the "wrong" data from being shared but focused on ensuring that the focus be on technical data corruption (rather a reluctance to map and interpret EHI) and/or for incorrect patient data when appropriate standards and best practices for patient matching is utilized. That is, an actor's failure to implement appropriate software which prevents the potential of corrupted data or mismatched data should not be used to justify this exception. If data corruption results in the infeasibility or downtime of the system, we would recommend deferring to those exceptions. In addition, language around lack of interpretability of data is not data corruption and may be addressed in another exception. Finally, the inclusion of an opportunity for clinicians to document why information sharing may result in harm is critical in adolescent medicine, behavioral health, infectious diseases, etc. where complexities of local policies, state law and existing federal law about the role of the clinician in determining what information may be withheld in the patient's (or another person's) best interest. The reasons for not sharing information under this exception of harm must be clearly documented within the EHR, the content of which must be made available by the vendor. The documentation must include the reasoning and conditions applied and must be made available for other users of the system and the patient to ensure that this exception does not result in unintended consequences. It is recognized that this will require implementation activities from health IT vendors, and this should be reflected in the enforcement timeline for the final rule.

Recommendation 14

Modify the regulatory text in (a) to read "…arising from any of the following -- " prior to sub-items (1) – (3).

Recommendation 15

Modify the regulatory text in (a) (1) to read “Technically corrupt (defined as data that has lost its base integrity and is no longer understandable by the information technology system that created it) or inaccurate data accessed in a patient’s electronic health record for intent of access, exchange or use.”

Recommendation 16

Add to the regulatory text a sub-item (d) that the practice should be documented in the electronic health record or system recording the EHI by the appropriate user when the exception arising from using conditions (a) - (c) and must contain the reasoning and criteria used in the judgement of the user who is engaging in the practice under this exception.

Recommendation 17

The regulatory text in (b) is confusing; the word “practice” refers to the information blocking potentially occurring under an exception. Perhaps rephrasing “If the practice (referring to the permissible information blocking activity) relies on an organizational policy, the policy must be—".

Recommendation 18

Recommend adding a sub-item to the regulatory text in (b) that existing organizational policies should be reviewed by the organization for consistency with these regulations in order to prevent confusion and undue burden to providers.

Recommendation 19

Recommend adding clear guidance (in preamble) of when this exception should be used versus the exceptions for infeasibility and maintenance.

Recommendation 20**:** Consider adding examples of where exceptions related to preventing harm from corrupt or inaccurate data or incorrect patient identification may interact with the exception for infeasibility.

## 8. Promoting the Privacy of EHI

The IBTF believes that legitimate privacy concerns are a sound basis for an exception to the information blocking provision. However, the IBTF, after much discussion, believes that the following recommendations should be incorporated into the final rule:

Recommendation 21

The Task Force **recommends** adding language indicating that organizational policies must comply with federal, state, and local laws.

Recommendation 22

The Task Force **recommends** that in section (b)(2) express consent (or dissent) should be documented and recorded.

Recommendation 23

The Task Force **recommends** that in section (c)(3) the reference to "meaningful" is replaced with "clear and prior notice."

Recommendation 24

The Task Force **recommends** that organizational practices that are extra to HIPAA or other relevant legislation should clearly be forbidden. For example, policies that restrict transmission to individuals via email where such is the requested form and format of access. In many cases documented organizational policies are used to deny access where access is required.

Recommendation 25

The Task Force **recommends** that the final rule should specify that organizations should implement policies which ensure compliance with patient consent to information sharing (or lack of information sharing).

Recommendation 26

The Task Force **recommends** that if an actor functions in multiple states, some of which have more restrictive laws, the actor should implement policies and procedures that accommodate those more restrictive laws only in circumstances where they are required and not extend those greater restrictions to situations where they are not required by law.

## 9. Promoting the Security of EHI

The Task Force is concerned that actors may leverage this exception to effect information blocking, masquerading as a legitimate concern to protect the integrity of patient information.

Recommendation 27

The Task Force **recommends** that if the entity requesting patient information can be reasonably considered "legitimate" in that they have passed relevant authentication mechanisms and can reasonably be considered to have appropriate organizational policies in place to protect patient

information, then ignorance of that requestor's specific controls is no reason to claim this exception.

Recommendation 28

The Task Force **recommends** modifying the regulatory text to reflect that if the requestor is the patient (data subject) themselves, and the patient is fully informed to the risks of their information not being appropriately secured, this exception cannot be claimed.

Recommendation 29

The Task Force **recommends** that actors should not have flexibility to adopt security practices, even when grounded in some standard, that are commercially unreasonable relative to leading practices for sensitive data, in ways that limit and restrict access to data for permissible purposes, unless there is some overriding legal obligation. As an example, although FedRAMP High or SRG High are defined standards, requiring FedRAMP High ATO as a standard for any data requester would serve to limit interoperability, unless there were some overriding security concern (e.g., MHS or VHA records that contain data relevant to national security).

## 10. Recovering Costs Reasonable Incurred

The Task Force believes there will be a high practical burden to apply the combination of 171.204 and 171.206 to determine appropriate fee structures. By splitting discussion about fees over two exceptions, the proposed regulatory text obscures the critical decision of which fees are permissible and impermissible.

While the Task Force understands the intent of ONC was to address problematic pricing behavior by discouraging rent seeking behavior and extractive pricing, while providing for market-based pricing to allow innovation, the Task Force believes the net force of the proposed rule will be to raise prices (by raising compliance burdens, such as accounting controls, pricing controls, and other pricing compliance activities) and limit the supply for value-added interoperability services.

The combination of the broad definition of EHI, the broad definition of HIN, and the unlimited applicability for 171.204 and 171.206 for all actors and all access, exchange and use, has the effect of putting nearly all interoperability products and services under Federal price controls. This approach lumps all interoperability in the category of problematic rent-seeking behavior requiring regulation. It places, for example, standards-based EHR interoperability interfaces, where high prices disincentive access and discourage an actor from making interfaces self-service; and innovative services, such as patient comparison shopping and bill payment, or AI-based risk scoring on exactly the same footing. The Task Force believes this sets the price for

interoperability that should be built-in too high; whereas it discourages value-added services from discovering the appropriate market-based price.

The Task Force finds that pricing related to **access** to what various members term the "legal medical record", "Designated Record Set" and/or the raw data of the record (and additional data used as part of the legal medical record to provide decision-making) is the most problematic with respect to information blocking. The Task Force also finds that Intellectual Property Rights (IPR) essential to basic access are critical; we accordingly believe that pricing regulation should be targeted to those fees that impede what might be termed "basic" access. The Task Force believes that basic access should be defined as activities essential to represent and interpret clinical, pricing, and related data in certified exchange standards.

Along these lines, the Task Force discussed the term "reasonable" with respect both to IPR (171.206) and cost-based pricing (171.204). The Task Force believes that what is "reasonable" varies according to the type and class of interoperability capability; in particular the Task Force believes that a lower fee (in many cases, a fee of zero) is "reasonable" for essential capabilities that define certified standards-based exchange of the legal medical record held, for example, in an EHR; in other cases, such as for value-added services not essential for basic access, or essential for ordinary exchange and use, what is "reasonable" should be defined by market mechanism.

The Task Force believes the applicability of 171.206 to licensed IPR and 171.204 for all other services creates a market distorting distinction between licensed products (e.g., software supplied on-prem as object code) and cloud-deployed software-as-a-service, which has a usage fee, but not a licensing fee. As more software moves to a cloud-deployed model, this market distortion is problematic.

In addition, the Task Force found some of the draft language confusing in practice or substantially disagreeing from usual practice.

For example, 171.204 speaks of "cost recovery" but the preamble implies reasonable profits are intended to be allowed. The usual terms for a pricing mechanism based on costs with target margin would be "cost-based pricing" or "cost-plus pricing" or "cost recovery with reasonable margin".

The term "non-standard" (although taken directly from the Cures Act legislative text) creates confusion between "does not conform to standards" and "implemented in a way that creates difficulty to interoperate".

The discussion in 171.204(c)(2) is confusingly worded. The Task Force believes the intent is to count only the direct costs of implementing interoperability.

Recommendation 30

The Task Force **recommends** that ONC combine the regulatory text currently supplied for 171.204 and 206 into a single allowed fee exception that clearly defines allowed and disallowed fee categories.

Recommendation 31

The Task Force **recommends** ONC use terminology that distinguishes between pure cost or expense recovery with no provision for margin or profit where this is intended and use terms such as "cost-based pricing" where margin or profit is allowed and "market-based pricing" where no restrictions on pricing are needed.

Recommendation 32

Where cost-based pricing mechanism are required, the Task Force **recommends** that the method for assessing the cost basis be reasonably associated with the complexity or cost of providing capabilities. Such methods could include reasonable heuristics, estimates or other commonly used methods. For example, size of organization, as measured in revenue or operating expense, is a commonly used heuristic to define pricing for exchange services, because revenue/expense is commonly available and directly correlated with patient flow, which is directly correlated with data volumes. Requiring activity-based accounting mechanism sufficient to account for the direct cost of providing, e.g., access services, is burdensome and is not a common or usual accounting practice. The Task Force believes that reasonable heuristics or estimates are sufficient to avoid arbitrary fees that could constitute information blocking without placing undue burden on actors.

Recommendation 33

The Task Force **recommends** that ONC distinguish between **Basic Access** and **Value-Added** Access, Exchange, and Use. Within this recommendation references to Designated Record Set and Covered Entity are interpreted in line with 45 CFR 164.501.

The IBTF suggests that ONC consider the following definitions appropriate:

- **Basic Access** where:
    - If an entity is considered a Covered Entity, information that is included within the Designated Record Set as defined in 45 CFR 164.501; or
    - If an entity is a Provider that is not a Covered Entity, the Designated Record Set as defined in 45 CFR 164.501; or

- If an entity is considered a HIE, HIN, or developer of health information technology, the information that was collected on behalf of a Covered Entity or non-Covered Entity; and

- Basic transformation of data required to implement standards (from the core standards list) reasonably required to enable exchange or implement the intended use of a certified technology.

- ***Value-Added Access***, exchange and use not included in Basic Access above.

  For example, infrastructural systems, capabilities that translate, transform, localize, perform decision support, complex transformations, or use artificial intelligence or machine learning, provide novel renderings of data, etc.

The IBTF notes that the emergent definition of USCDI may provide a useful definitional basis for Basic and Value Added access in the future.

Recommendation 34

Notwithstanding the recommended distinction between basic and value-added capabilities, the Task Force **recommends** that when the output of value-added services are incorporated into, or form, an essential part of the legal medical record, or are routinely used for decision making, they constitute part of the set to which basic access is required (e.g., if a vendor supplies clinical risk scoring services based on the basic record, those services may be offered at market rates; if the risk score is incorporated into or used by clinical staff to make clinical decisions, the individual risk score accordingly becomes part of the record and forms part of basic access to which basic access fee regulation is applied).

Recommendation 35

The Task Force **recommends** that ONC distinguish between IPR that are ***essential*** to access and IPR that allow for value-added services. The former would include standards-essential IPR or any IPR licensing associated with terminology either defined in certified standards or reasonably required based on regulatory requirements or customary use.

Recommendation 36

The Task Force **recommends** that allowed fees for basic access be on a pure direct cost recovery basis only. In many cases, where basic access is provided via widely deployed consensus-based certified standards built into health IT, such direct costs would be minimal.

The Task Force does **not recommend** that the cost to develop standards be part of the cost basis for fees for basic access; rather any such costs should be a part of the fees for the health IT. The Task Force believes this approach provides a significant incentive to adopt standards; actors who do not provide access through widely deployed consensus-based standards would have an incentive to do so to reduce the total cost structure of access. The Task Force **recommends** that the cost basis for fees basic access **not** include reasonable mapping to standards (that is, such one-time costs would be a cost of producing Health IT, not a cost of access); such mapping would include mapping of proprietary terminologies used internally to the standard terminologies used externally (e.g., internal problem list terminologies to SNOMED CT, or proprietary medication databases to RxNorm). Exceptions would include cases where data or terminology sets exist that are not reasonable to include in mapping to standards AND where sufficient mechanisms of basic access exposing the non-standard data exist. In these cases, there are market-based mechanism (e.g., systems integrators) sufficient to set prices for non-standard data mapping.

Recommendation 37

The Task Force **recommends** that allowed fees for access, exchange and use essential IPR be set on a RAND-basis. Such fees would not be "reasonable" if they materially discourage access, exchange or use, or impede the development of competitive markets for value-added exchange and use services. The Task Force **recommends** that access, exchange and use-essential IPR license grants be sufficient for actors to provide access and/or deliver exchange and use services; for example, IPR grants for terminology sets that are access, exchange and use essential should be sufficient to allow access, exchange and use for permissible purposes. To put this another way, actors would not be able to accept IPR licenses that restrict access only those who also have IPR rights.

Recommendation 38

The Task Force **recommends** no further restrictions on permitted fees; the Task Force believes that the above restrictions on permitted fees are sufficient to address monopoly rents or gatekeepers and enable market-based pricing for additional services.

## 11. Responding to Requests that are Infeasible

The Task Force feels that this exception must not be used simply because it would be inconvenient, or have some limited cost, to comply with regulation. The Task Force makes some minor suggestions to aid the drafting of this exception as detailed below.

Recommendation 39

| ORIGINAL | RECOMMENDED REGULATION TEXT | COMPARISON / MARKUP |
|---|---|---|
| To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.<br><br>(a) *Request is infeasible*.<br>(1) The actor must demonstrate, in accordance with paragraph (a)(2) of this section, that complying with the request in the manner requested would impose a substantial burden on the actor that is unreasonable under the circumstances, taking into consideration—<br>(i) The type of electronic health information and the purposes for which it may be needed;<br>(ii) The cost to the actor of complying with the request in the manner requested;<br>(iii) The financial, technical, and other resources available to the actor;<br>(iv) Whether the actor provides comparable access, exchange, or use to itself or to its customers, suppliers, partners, and other persons with whom it has a business relationship;<br>(v) Whether the actor owns or has control over a predominant technology, platform, health information exchange, or health information network through which electronic health information is accessed or exchanged;<br>(vi) Whether the actor maintains electronic protected health information on behalf of a covered entity, as defined in 45 CFR 160.103, or maintains electronic health information on behalf of the requestor or another person whose access, exchange, or use of electronic health information will be enabled or facilitated by the actor's compliance with the request; | To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.<br><br>(a) *Request is infeasible*.<br>(1) The actor must demonstrate, in accordance with paragraph (a)(2) of this section, that complying with the request in the manner requested would impose a substantial burden on the actor that is unreasonable under the circumstances, taking into consideration—<br>(i) The type of electronic health information and the purposes for which it may be needed;<br>(ii) The cost to the actor of complying with the request in the manner requested;<br>(iii) The financial, technical, and other resources available to the actor;<br>(iv) Whether the actor provides comparable access, exchange, or use to itself or to its customers, suppliers, partners, and other persons with whom it has a business relationship;<br>(v) Whether the actor owns or has control over a predominant technology, platform, health information exchange, or health information network through which electronic health information is accessed or exchanged;<br>(vi) Whether the actor maintains electronic protected health information on behalf of a covered entity, as defined in 45 CFR 160.103, or maintains electronic health information on behalf of the requestor or another person whose access, exchange, or use of electronic health information will be enabled or facilitated by the actor's compliance with the request; | To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.<br><br>(a) *Request is infeasible*.<br>(1) The actor must demonstrate, in accordance with paragraph (a)(2) of this section, that complying with the request in the manner requested would impose a substantial burden on the actor that is unreasonable under the circumstances, taking into consideration—<br>(i) The type of electronic health information and the purposes for which it may be needed;<br>(ii) The cost to the actor of complying with the request in the manner requested;<br>(iii) The financial, technical, and other resources available to the actor;<br>(iv) Whether the actor provides comparable access, exchange, or use to itself or to its customers, suppliers, partners, and other persons with whom it has a business relationship;<br>(v) Whether the actor owns or has control over a predominant technology, platform, health information exchange, or health information network through which electronic health information is accessed or exchanged;<br>(vi) Whether the actor maintains electronic protected health information on behalf of a covered entity, as defined in 45 CFR 160.103, or maintains electronic health information on behalf of the requestor or another person whose access, exchange, or use of electronic health information will be enabled or facilitated by the actor's compliance with the request; |

| | | |
|---|---|---|
| (vii) Whether the requestor and other relevant persons can reasonably access, exchange, or use the electronic health information from other sources or through other means; and<br>(viii) The additional cost and burden to the requestor and other relevant persons of relying on alternative means of access, exchange, or use.<br>(2) The following circumstances do not constitute a burden to the actor for purposes of this exception and shall not be considered in determining whether the actor has demonstrated that complying with a request would have been infeasible.<br>(i) Providing the requested access, exchange, or use in the manner requested would have facilitated competition with the actor.<br>(ii) Providing the requested access, exchange, or use in the manner requested would have prevented the actor from charging a fee.<br><br>(b) *Responding to requests*. The actor must timely respond to all requests relating to access, exchange, or use of electronic health information, including but not limited to requests to establish connections and to provide interoperability elements.<br><br>(c) *Written explanation*. The actor must provide the requestor with a detailed written explanation of the reasons why the actor cannot accommodate the request.<br><br>(d) *Provision of a reasonable alternative*. The actor must work with the requestor to identify and provide a reasonable alternative means of accessing, exchanging, or using the electronic health information. | (vii) whether similarly situated actors provide similar access, exchange or use;<br>(viii) Whether the requestor and other relevant persons can reasonably access, exchange, or use the electronic health information from other sources or through other means; and<br>(viiii) The additional cost and burden to the requestor and other relevant persons of relying on alternative means of access, exchange, or use.<br>(2) The following circumstances do not constitute a burden to the actor for purposes of this exception and shall not be considered in determining whether the actor has demonstrated that complying with a request would have been infeasible.<br>(i) Providing the requested access, exchange, or use in the manner requested would have facilitated competition with the actor.<br>(ii) Providing the requested access, exchange, or use in the manner requested would have prevented the actor from charging a fee.<br><br>(b) *Responding to requests*. The actor must respond to all requests relating to access, exchange, or use of electronic health information, including but not limited to requests to establish connections and to provide interoperability elements in a timely manner under the circumstances which shall not exceed 10 business days. Such response shall include a detailed written explanation of the reasons why the actor cannot accommodate the request.<br><br>(c) *Provision of a reasonable alternative*. The actor must work with the requestor in a timely manner to identify and provide a reasonable alternative means of | (vii) whether similarly situated actors provide similar access, exchange or use;<br>(viii)~~(vii)~~ Whether the requestor and other relevant persons can reasonably access, exchange, or use the electronic health information from other sources or through other means; and<br>(viiii)~~(viii)~~ The additional cost and burden to the requestor and other relevant persons of relying on alternative means of access, exchange, or use.<br>(2) The following circumstances do not constitute a burden to the actor for purposes of this exception and shall not be considered in determining whether the actor has demonstrated that complying with a request would have been infeasible.<br>(i) Providing the requested access, exchange, or use in the manner requested would have facilitated competition with the actor.<br>(ii) Providing the requested access, exchange, or use in the manner requested would have prevented the actor from charging a fee.<br><br>(b) *Responding to requests*. The actor must ~~timely~~ respond to all requests relating to access, exchange, or use of electronic health information, including but not limited to requests to establish connections and to provide interoperability elements in a timely manner under the circumstances which shall not exceed 10 business days. Such response shall include ~~(c) *Written explanation*. The actor must provide the requestor with~~ a detailed written explanation of the reasons why the actor cannot accommodate the request.<br><br>(~~d~~c) *Provision of a reasonable alternative*. The actor must work |

| | | |
|---|---|---|
| | accessing, exchanging, or using the electronic health information as applicable. | with the requestor in a timely manner to identify and provide a reasonable alternative means of accessing, exchanging, or using the electronic health information as applicable. |

## 12. Licensing of Interoperability Elements on RAND Terms

The Task Force spent considerable time discussing and expounding the RAND terms as reasons for legitimate exceptions. In conjunction with the preamble, the Task Force felt that the majority of the regulation text as drafted was appropriate, and had minor recommendations concerning intent and clarity as detailed below.

Recommendation 40

| ORIGINAL | RECOMMENDED REGULATION | COMPARISON / MARKUP |
|---|---|---|
| To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.<br><br>(a) *Responding to requests*. Upon receiving a request to license or use interoperability elements, the actor must respond to the requestor within 10 business days from receipt of the request by:<br>(1) Negotiating with the requestor in a reasonable and non-discriminatory fashion to identify the interoperability elements that are needed; and<br>(2) Offering an appropriate license with reasonable and non-discriminatory terms.<br><br>(b) *Reasonable and non-discriminatory terms*. The actor must license the interoperability elements described in paragraph (a) of this section on terms that are reasonable and non-discriminatory.<br>(1) *Scope of rights*. The license must provide all rights necessary to access | To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.<br><br>(a) *Responding to requests*. Upon receiving a request to license or use interoperability elements, the actor must respond to the requestor within 10 business days from receipt of the request by:<br>(1) Negotiating with the requestor in a reasonable and non-discriminatory fashion to identify the interoperability elements that are needed;<br>(2) Offering an appropriate license with reasonable and non-discriminatory terms; and<br>(3) Beginning negotiations with the intent to furnish a quotation for a license<br><br>(b) *Reasonable and non-discriminatory terms*. The actor must license the interoperability elements described in paragraph (a) of this section on terms that are reasonable and non-discriminatory. | To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.<br><br>(a) *Responding to requests*. Upon receiving a request to license or use interoperability elements, the actor must respond to the requestor within 10 business days from receipt of the request by:<br>(1) Negotiating with the requestor in a reasonable and non-discriminatory fashion to identify the interoperability elements that are needed;<br>(2) Offering an appropriate license with reasonable and non-discriminatory terms; and<br>(3) Beginning negotiations with the intent to furnish a quotation for a license<br><br>(b) *Reasonable and non-discriminatory terms*. The actor must license the interoperability elements described in paragraph (a) of this section on terms that are reasonable and non-discriminatory. |

| | | |
|---|---|---|
| and use the interoperability elements for the following purposes, as applicable.<br>(i) Developing products or services that are interoperable with the actor's health IT, health IT under the actor's control, or any third party who currently uses the actor's interoperability elements to interoperate with the actor's health IT or health IT under the actor's control.<br>(ii) Marketing, offering, and distributing the interoperable products and/or services to potential customers and users.<br>(iii) Enabling the use of the interoperable products or services in production environments, including accessing and enabling the exchange and use of electronic health information. | (1) *Scope of rights*. The license must provide all rights necessary to access and use the interoperability elements for the following purposes, as applicable.<br>(i) Developing products or services that are interoperable using the licensed interoperability elements<br>(ii) Marketing, offering, and distributing the interoperable products and/or services to potential customers and users.<br>(iii) Enabling the use of the interoperable products or services in production environments, including accessing and enabling the exchange and use of electronic health information. | (1) *Scope of rights*. The license must provide all rights necessary to access and use the interoperability elements for the following purposes, as applicable.<br>(i) Developing products or services that are interoperable ~~with the actor's health IT, health IT under the actor's control, or any third party who currently~~ us~~es~~ing the licensed ~~actor's~~ interoperability elements ~~to interoperate with the actor's health IT or health IT under the actor's control.~~<br>(ii) Marketing, offering, and distributing the interoperable products and/or services to potential customers and users.<br>(iii) Enabling the use of the interoperable products or services in production environments, including accessing and enabling the exchange and use of electronic health information. |

## 13. Maintaining and Improving Health IT Performance

Recommendation 41

The Task Force recommends that ONC generalize the maintenance exception to cover the following:

- Rate limiting or disabling use of the health IT by user or actors whose use is unusual or would cause degradation of overall performance
- Reasonable and usual practices where SLA or maintenance windows are not named in contract
- Out of SLA performance with reasonable good-faith activity to restore service in a timely matter
- Force majeure or other highly unusual events out of the control of the actor.

Failure to consider these exceptions raises the risk that ordinary failures to achieve good faith service restoration would be adjudicated as information blocking, rather than through normal contractual resolution processes, and would create a paradoxical incentive for actors to insist on negotiating lower SLA achievement targets.

While we understand that some actors have caused information blocking by abandoning technology, we believe such instances are rare and would not trigger the exceptions noted above.

Recommendation 42

| ORIGINAL | RECOMMENDED REGULATION | COMPARISON / MARKUP |
|---|---|---|
| To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.<br>(a) Maintenance and improvements to health IT. An actor may make health IT under its control temporarily unavailable in order to perform maintenance or improvements to the health IT, provided that the actor's practice is—<br>(1) For a period of time no longer than necessary to achieve the maintenance or improvements for which the health IT was made unavailable; | To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.<br>(a) *Maintenance and improvements to health IT*. An actor may make health IT under its control temporarily unavailable in order to perform maintenance or improvements to the health IT, provided that the actor's practice is—<br>(1) a reasonable, good-faith activity lasting a period of time no longer than necessary to achieve the maintenance or improvements for which the health IT was made unavailable; and | To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.<br>(a) *Maintenance and improvements to health IT*. An actor may make health IT under its control temporarily unavailable in order to perform maintenance or improvements to the health IT, provided that the actor's practice is—<br>(1) a reasonable, good-faith activity lasting ~~For~~ a period of time no longer than necessary to achieve the maintenance or improvements for which the health IT was made unavailable; and |

| | | |
|---|---|---|
| (2) Implemented in a consistent and non-discriminatory manner; and<br>(3) If the unavailability is initiated by a health IT developer of certified health IT, HIE, or HIN, agreed to by the individual or entity to whom the health IT developer of certified health IT, HIE, or HIN supplied the health IT.<br><br>(b) Practices that prevent harm. If the unavailability of health IT for maintenance or improvements is initiated by an actor in response to a risk of harm to a patient or another person, the actor does not need to satisfy the requirements of this section, but must comply with all requirements of § 171.201 at all relevant times to qualify for an exception.<br><br>(c) Security-related practices. If the unavailability of health IT for maintenance or improvements is initiated by an actor in response to a security risk to electronic health information, the actor does not need to satisfy the requirements of this section, but must comply with all requirements of § 171.203 at all relevant times to qualify for an exception. | (2) Implemented in a consistent and non-discriminatory manner.<br><br>(b) *Practices that prevent harm.* If the unavailability of health IT for maintenance or improvements is initiated by an actor in response to a risk of harm to a patient or another person, the actor does not need to satisfy the requirements of this section, but must comply with all requirements of § 171.201 at all relevant times to qualify for an exception.<br><br>(c) *Security-related practices*. If the unavailability of health IT for maintenance or improvements is initiated by an actor in response to a security risk to electronic health information, the actor does not need to satisfy the requirements of this section, but must comply with all requirements of § 171.203 at all relevant times to qualify for an exception.<br><br>(d) *Responding to requests that are infeasible.* If the unavailability of health IT is due to highly unusual events out of the control of the actor such as a natural disaster, the actor does not need to satisfy the requirements of this section, if the practice complies with all requirements of §171.205. | (2) Implemented in a consistent and non-discriminatory manner~~.; and~~<br>~~(3) If the unavailability is initiated by a health IT developer of certified health IT, HIE, or HIN, agreed to by the individual or entity to whom the health IT developer of certified health IT, HIE, or HIN supplied the health IT.~~<br><br>(b) *Practices that prevent harm.* If the unavailability of health IT for maintenance or improvements is initiated by an actor in response to a risk of harm to a patient or another person, the actor does not need to satisfy the requirements of this section, but must comply with all requirements of § 171.201 at all relevant times to qualify for an exception.<br><br>(c) *Security-related practices*. If the unavailability of health IT for maintenance or improvements is initiated by an actor in response to a security risk to electronic health information, the actor does not need to satisfy the requirements of this section, but must comply with all requirements of § 171.203 at all relevant times to qualify for an exception.<br><br>(d) *Responding to requests that are infeasible.* If the unavailability of health IT is due to highly unusual events out of the control of the actor such as a natural disaster, the actor does not need to satisfy the requirements of this section, if the practice complies with all requirements of §171.205. |

## 14. Additional Exceptions (Request for Information)

Contractual obligations may and often do conflict with the broad requirements for information blocking. The preamble text discusses multiple situations where contractual terms are used by actors to restrict use of information. The preamble did not address situations where actors are dependent on contractual terms from other parties that may conflict with information blocking provisions.

As an example, business associates (BAs) have only the data use rights that are granted under a business associate agreement (BAA); these data use rights may not allow access for all permissible uses. Contractual terms that limit BA data use rights are quite common. Should counterparties not change BAA terms, BAs would be in a difficult position, forced to choose between:

- Cancelling contracts, often subjecting BAs to penalties under contract, and sometimes opening BAs to information blocking enforcement;
- Complying with contractual terms and risking information blocking enforcement;
- Complying with information blocking provisions, while violating contracts and possibly opening HHS OCR enforcement for violating BAA terms.

In other examples, confidentiality provisions of contracts have been used to litigate data use for price transparency, even when such data use is permitted by data use terms in BAAs.

Similar situations would apply for IPR licenses (e.g., terminology sets) that may have provisions preventing information sharing with information requesters who do not have IPR grants.

Recommendation 43

The Task Force **recommends** that the status of contractual obligations that may be in conflict with information blocking obligations be explicitly clarified by ONC as being void. The simplest solution would be to interpret the intent of Congress to preempt specific contractual terms that are in conflict with the Cures Act.

Recommendation 44

*Trusted Exchange Framework and Common Agreement*

In ONC's Proposed Rule, ONC noted that they are considering whether they should propose, in a future rulemaking, a narrow exception to the information blocking provision for practices that are necessary to comply with the requirements of the Common Agreement (CA). The release of the

second draft of the Trusted Exchange Framework (TEF) late in the public consultation period for the Proposed Rule has given the IBTF the opportunity to comment upon the TEF and the CA.

Considerable discourse has taken place, with two distinct views being articulated:

- That compliance with the TEF should provide a "safe lane" which demonstrates to ONC/HHS Office of Inspector General (OIG) that information blocking is not taking place; and

- That providing a "safe lane" is a protectionist approach which should not be adopted and the TEF should be a series of good practice guidelines.

We urge ONC during the rulemaking process to consider carefully the enduring demand of the Cures Act to promote information sharing and prohibit information blocking amongst all actors involved in the provision and administration of care. We believe that a careful balance needs to be struck to encourage compliance to the information blocking provision, potentially through adoption of the TEF, and the need to investigate information blocking activities where warranted – and not inadvertently provide bad actors with an opportunity to circumvent regulation compliance.

## 15. Complaint Process

The IBTF supports ONC's proposal on the information blocking complaint process as it is written in the Proposed Rule with no further edits or comments.

## 16. Disincentives for Health Care Providers (Request for Information)

The Task Force believes that, while some types of problematic activities relating to information blocking are more typical of health IT developers or other similar actors, other refusals to share data, including using over interpretation of HIPAA and other privacy laws, stricter than necessary organizational policies, or concerns of patient "leakage" to competitive institutions, are more typical of provider organizations. The IBTF believes that disincentives must be sufficient to discourage problematic behavior, encourage compliance, and incent providers to work with OIG and others to address and remediate problematic behavior.

Recommendation 45

The Task Force **recommends** that ONC work with CMS to build information blocking disincentives into a broad range of CMS programs, and that ONC work with other Federal departments and agencies that contract with providers (e.g., VHA, DoD MHS, IHS, CDC, etc.) to similarly build information blocking disincentives into contracting and other programs.

## Recommendation 46

The Task Force **recommends** that providers attest to comply with information blocking requirements as a part of Conditions of Participation, Conditions for Coverage, contracts, and other similar relationships, covering both FFS, value-based care, and direct payment relationships, and that findings of information blocking by OIG, findings violations relating to information blocking attestations of the False Claims Act by FTC, or other similar enforcement actions trigger disincentives up to and including removing organizations from participation or coverage.

## Conditions and Maintenance of Certification and Enforcement

### 17. 170.401 Information Blocking

The IBTF supports ONC's proposal on the Information Blocking Condition of Certification as it is written in the Proposed Rule with no further edits or comments.

### 18. 170.402 Assurances

The Task Force considered this Condition of Certification and Maintenance of Certification for certified health IT at length. Discussions focused upon the transparency of the certification process, recommendations concerning "honesty" in communications by a vendor, and mandating the Certified Health IT Product List (CHPL) for publishing product certification periods have been made. In addition, setting a minimum retention period for record keeping in the event that an IT vendor removes a product from market was felt to be appropriate to ensure that potentially short lived products would inadvertently not have their documentation maintained.

Recommendation 47

| ORIGINAL | RECOMMENDED REGULATION | COMPARISON / MARKUP |
|---|---|---|
| (a) *Condition of Certification.*<br><br>(1) A health IT developer must provide assurances satisfactory to the Secretary that the health IT developer will not take any action that constitutes information blocking as defined in 42 U.S.C. 300jj-52 and § 171.103, unless for legitimate purposes specified by the Secretary; or any other action that may inhibit the appropriate exchange, access, and use of electronic health information.<br><br>(2) A health IT developer must ensure that its health IT certified under the ONC Health IT Certification Program conforms to the full scope of the certification criteria.<br><br>(3) A health IT developer must not take any action that could interfere with a user's ability to access or | (a) *Condition of Certification.*<br><br>(1) A health IT developer must provide assurances satisfactory to the Secretary that the health IT developer will not take any action that constitutes information blocking as defined in 42 U.S.C. 300jj-52 and § 171.103, unless for legitimate purposes specified by the Secretary; or any other action that may inhibit the appropriate exchange, access, and use of electronic health information.<br><br>(2) A health IT developer must ensure that its health IT certified under the ONC Health IT Certification Program conforms to the full scope of the certification criteria.<br><br>(3) A health IT developer must not take any action that could interfere with a user's ability to access or | (a) *Condition of Certification.*<br><br>(1) A health IT developer must provide assurances satisfactory to the Secretary that the health IT developer will not take any action that constitutes information blocking as defined in 42 U.S.C. 300jj-52 and § 171.103, unless for legitimate purposes specified by the Secretary; or any other action that may inhibit the appropriate exchange, access, and use of electronic health information.<br><br>(2) A health IT developer must ensure that its health IT certified under the ONC Health IT Certification Program conforms to the full scope of the certification criteria.<br><br>(3) A health IT developer must not take any action that could interfere with a user's ability to access or |

| | | |
|---|---|---|
| use certified capabilities for any purpose within the scope of the technology's certification.<br><br>(4) A health IT developer that manages electronic health information must certify health IT to the certification criterion in § 170.315(b)(10).<br><br>(b) *Maintenance of Certification*.<br><br>(1) A health IT developer must retain all records and information necessary to demonstrate initial and ongoing compliance with the requirements of the ONC Health IT Certification Program for: (i) A period of 10 years beginning from the date each of a developer's health IT is first certified under the Program; or (ii) If for a shorter period of time, a period of 3 years from the effective date that removes all of the certification criteria to which the developer's health IT is certified from the Code of Federal Regulations.<br>(2) A health IT developer that must comply with the requirements of paragraph (a)(4) of this section must provide all of its customers of certified health IT with the health IT certified to the certification criterion in § 170.315(b)(10) within 24 months of this final rule's effective date or within 12 months of certification for a health IT developer that never previously certified health IT to the 2015 Edition, whichever is longer. | use certified capabilities for any purpose within the scope of the technology's certification, and the health IT developer shall provide honest communication and expert advice as required by a user.<br><br>(4) A health IT developer that manages electronic health information must certify health IT to the certification criterion in § 170.315(b)(10).<br><br>(b) *Maintenance of Certification*.<br><br>(1) A health IT developer must retain all records and information necessary to demonstrate initial and ongoing compliance with the requirements of the ONC Health IT Certification Program for:<br><br>(i) A period of 10 years beginning from the date each of a developer's health IT is first certified under the Program; or<br><br>(ii) If for a shorter period of time, a period of 3 years from the effective date that removes all of the certification criteria to which the developer's health IT is certified from the Code of Federal Regulations.<br><br>(iii) If for a shorter period of time, a period of 3 years from the date of withdrawal by the health IT developer of a certified health IT product from certification.<br><br>(2) A health IT developer that must comply with the requirements of paragraph (a)(4) of this section must provide all of its customers of certified health IT with the health IT certified to the certification criterion in § 170.315(b)(10) within:<br><br>(i) 24 months of this final rule's effective date, or | use certified capabilities for any purpose within the scope of the technology's certification~~.~~, and the health IT developer shall provide honest communication and expert advice as required by a user.<br><br>(4) A health IT developer that manages electronic health information must certify health IT to the certification criterion in § 170.315(b)(10).<br><br>(b) *Maintenance of Certification*.<br><br>(1) A health IT developer must retain all records and information necessary to demonstrate initial and ongoing compliance with the requirements of the ONC Health IT Certification Program for:<br><br>(i) A period of 10 years beginning from the date each of a developer's health IT is first certified under the Program; or<br><br>(ii) If for a shorter period of time, a period of 3 years from the effective date that removes all of the certification criteria to which the developer's health IT is certified from the Code of Federal Regulations.<br><br>(iii) If for a shorter period of time, a period of 3 years from the date of withdrawal by the health IT developer of a certified health IT product from certification.<br><br>(2) A health IT developer that must comply with the requirements of paragraph (a)(4) of this section must provide all of its customers of certified health IT with the health IT certified to the certification criterion in § 170.315(b)(10) within:<br><br>(i) 24 months of this final rule's effective date, or |

| | | |
|---|---|---|
| | (ii) 12 months of certification for a health IT developer that never previously certified health IT to the 2015 Edition.<br><br>(3) ONC will preserve on the CHPL (or in another format) a list of the start and end dates of each previously certified health IT product. | (ii) ~~within~~ 12 months of certification for a health IT developer that never previously certified health IT to the 2015 Edition.~~, whichever is longer.~~<br><br>(3) ONC will preserve on the CHPL (or in another format) a list of the start and end dates of each previously certified health IT product. |

## 19. 170.402 Assurances – Request for Information Regarding the Trusted Exchange Framework and the Common Agreement

Recommendation 48

[This recommendation has been removed.]

## 20. 170.403 Communications

Recommendation 49

There was concern in the IBTF that ONC's timeline for updates to contracts was insufficient and that the work was significantly underestimated by ONC's regulatory impact analysis. There was an example raised from a member of the group of needing to hire four additional lawyers to complete the work in that timeframe. The intent was to instead have health IT developers propose a plan for contract updates in 2 years, and update contracts at next renewal or within 5 years.

The Task Force recommends the following revisions to the regulatory text:

(2) Contracts and agreements.

(i) A health IT developer must not establish, renew, or enforce any contract or agreement that contravenes paragraph (a) of this section.

(ii) If a health IT developer has a contract or agreement in existence at the time of the effective date of this final rule that contravenes paragraph (a) of this section, then the developer must in a reasonable period of time, but not later than two years from the effective date of this rule, ~~amend the contract or~~ agree with the relevant client on a plan to amend the contract or an agreement to

remove or void the contractual provision that contravenes paragraph (a) of this section.

(iii) The plan required by paragraph (ii) of this section must be completed within five years of the effective date of this rule.

Recommendation 50

It was discussed that attempting to enumerate on a screen what might be third-party content that was the intellectual property of a third party was infeasible. Instead, health IT developers could provide a list of third-party content that might be present.

The Task Force recommends the following revisions to the regulatory text:

(iii) The developer has put all potential communicators on sufficient written notice of a list of third-party content included in the health IT ~~each aspect of its screen display that contains third-party content~~ that cannot be communicated because the reproduction would infringe the third-party's intellectual property rights;

Recommendation 51

There was discussion of whether administrative functions of health IT could unintentionally reveal significant intellectual property of health IT developers. For example, the security configuration of health IT is less important in meeting the needs of communications protected under the Cures Act.

The Task Force recommends clarifying in the preamble that appropriate administrative functions of health IT could be included as "non-user facing aspects" based on the assessment that those communications are not matching the purpose required by the Cures Act and that also affect a limited set of users.

Recommendation 52

There was discussion of concerns of sharing screenshots, the value that health IT developers put on time spent designing and improving screens and user interfaces, and that there are valid reasons why screenshots are both required to be shared and could also be considered "fair use." The goal was that the communications protected under the Cures Act should not permit unintended use, such as using screenshots to attempt to copy screen designs from a competitor. Some members of the Task Force felt that the "fair use" provisions of the preamble already prohibited copying for competitive reasons. However, the restriction that screenshots be permitted to be communicated under fair use principles is not in the regulatory text and the group felt that it deserved further consideration. The intent of the Task Force was that the

actor disclosing a screenshot is responsible for determining that the disclosure's purpose does meet the "fair use" expectations and that further redisclosures would have to similarly meet the fair use expectations, and in doing so appropriately protect from potential intellectual property infringements.

The Task Force recommends the following revisions to the regulatory text:

> (2) A health IT developer does not prohibit the fair use communication of screenshots of the developer's health IT, subject to the limited restrictions described in paragraph (a)(2)(ii)(D) of this section, and with the understanding that any actor disclosing the screenshots is responsible for communicating that each use is to be put to "fair use."

Recommendation 53

In (2)(i)(A), the group felt that it was reasonable for health IT developers to request that they be notified when a disclosure required by law takes place, and that this was accommodated in the current regulatory text.

Recommendation 54

In (2)(i)(C), the group felt that notification to health IT developers prior to (or simultaneous with, if prior was not possible) public reporting would be beneficial for resolving security vulnerabilities prior to the knowledge being widespread.

Recommendation 55

In (2)(i) the group felt that a specific protection might be called for those individuals who highlight information blocking practices and identify them to the appropriate authorities so that the individual is not subject to retaliatory action by the actor identified by the whistleblower. Obviously ONC would need to phrase it so that a whistleblower would not be able to leverage this as mechanism to avoid sanctions for other activities (e.g. performance etc.).

The Task Force recommends the following addition to regulatory text:

> (E) Communicating information about a health IT developer's failure to comply with a Condition of Certification, or with any other requirement of this part, to ONC or an ONC-ACB. Any person who makes a communication covered by (2)(i) to an appropriate entity must not be subject to retaliatory action which could reasonably be considered due to their whistleblowing activity.

Recommendation 56

The Task Force recommends an additional category of communications that would not be protected (neither receiving unqualified protection nor their restriction necessitating a permitted restriction). The intent was that this category would include communications such as false communications, things protected by attorney-client privilege, and so forth. The Task Force did not intend for false communications such as libel to be protected as an unintended consequence. Other examples of unprotected communications might include communications sent by a person who improperly obtained the information or received it from somebody who did not have the right to provide the information, such as a hacker.

The Task Force recommends clarifying in preamble that the goal of the unprotected communications provision is to not extend protections of necessitate permitted restrictions for this category of communications. Specifically, where a communication is unlawful (such as violations of securities law or court orders); the content is false, deceptive, or likely to cause confusion (such as trade libel or trademark infringement); the content is protected by law from disclosure (such as attorney-client privileged communications); the content is subject to a lawful obligation on the health IT developer to prohibit or restrict such communication (such as third party intellectual property); or the content was obtained without authorization (such as by a hacker).

The Task Force recommends the following addition to regulatory text:

> (a)(3) Unprotected Communications. Specific communications are not extended the protections or restrictions in this section, where those communications are considered unprotected in that they are either:
>
> (i) protected by other legislation or regulation; or
>
> (ii) false or unlawful.

Corresponding Suggested Regulatory Text Changes for the Above Recommendations

| ORIGINAL | RECOMMENDED REGULATION | COMPARISON / MARKUP |
|---|---|---|
| (a) *Condition of Certification*.<br><br>(1) A health IT developer may not prohibit or restrict the communication regarding—<br><br>(i) The usability of its health IT;<br>(ii) The interoperability of its health IT;<br>(iii) The security of its health IT; | (a) *Condition of Certification*.<br><br>(1) A health IT developer may not prohibit or restrict the communication regarding—<br><br>(i) The usability of its health IT;<br>(ii) The interoperability of its health IT;<br>(iii) The security of its health IT; | (a) *Condition of Certification*.<br><br>(1) A health IT developer may not prohibit or restrict the communication regarding—<br><br>(i) The usability of its health IT;<br>(ii) The interoperability of its health IT;<br>(iii) The security of its health IT; |

| | | |
|---|---|---|
| (iv) Relevant information regarding users' experiences when using its health IT;<br>(v) The business practices of developers of health IT related to exchanging electronic health information; and<br>(vi) The manner in which a user of the health IT has used such technology.<br><br>(2) A health IT developer must not engage in any practice that prohibits or restricts a communication regarding the subject matters enumerated in paragraph (a)(1) of this section, unless the practice is specifically permitted by this paragraph and complies with all applicable requirements of this paragraph.<br><br>(i) *Unqualified protection for certain communications.* A health IT developer must not prohibit or restrict any person or entity from communicating any information or materials whatsoever (including proprietary information, confidential information, and intellectual property) when the communication is about one or more of the subject matters enumerated in paragraph (a)(1) of this section and is made for any of the following purposes—<br><br>(A) Making a disclosure required by law;<br><br>(B) Communicating information about adverse events, hazards, and other unsafe conditions to government agencies, health care accreditation organizations, and patient safety organizations;<br><br>(C) Communicating information about cybersecurity threats and incidents to government agencies; | (iv) Relevant information regarding users' experiences when using its health IT;<br>(v) The business practices of developers of health IT related to exchanging electronic health information; and<br>(vi) The manner in which a user of the health IT has used such technology.<br><br>(2) A health IT developer must not engage in any practice that prohibits or restricts a communication regarding the subject matters enumerated in paragraph (a)(1) of this section, unless the practice is specifically permitted by this paragraph and complies with all applicable requirements of this paragraph.<br><br>(i) *Unqualified protection for certain communications.* A health IT developer must not prohibit or restrict any person or entity from communicating any information or materials whatsoever (including proprietary information, confidential information, and intellectual property) when the communication is about one or more of the subject matters enumerated in paragraph (a)(1) of this section and is made for any of the following purposes—<br><br>(A) Making a disclosure required by law;<br><br>(B) Communicating information about adverse events, hazards, and other unsafe conditions to government agencies, health care accreditation organizations, and patient safety organizations;<br><br>(C) Communicating information about cybersecurity threats and incidents to government agencies; | (iv) Relevant information regarding users' experiences when using its health IT;<br>(v) The business practices of developers of health IT related to exchanging electronic health information; and<br>(vi) The manner in which a user of the health IT has used such technology.<br><br>(2) A health IT developer must not engage in any practice that prohibits or restricts a communication regarding the subject matters enumerated in paragraph (a)(1) of this section, unless the practice is specifically permitted by this paragraph and complies with all applicable requirements of this paragraph.<br><br>(i) *Unqualified protection for certain communications.* A health IT developer must not prohibit or restrict any person or entity from communicating any information or materials whatsoever (including proprietary information, confidential information, and intellectual property) when the communication is about one or more of the subject matters enumerated in paragraph (a)(1) of this section and is made for any of the following purposes—<br><br>(A) Making a disclosure required by law;<br><br>(B) Communicating information about adverse events, hazards, and other unsafe conditions to government agencies, health care accreditation organizations, and patient safety organizations;<br><br>(C) Communicating information about cybersecurity threats and incidents to government agencies; |

| | | |
|---|---|---|
| (D) Communicating information about information blocking and other unlawful practices to government agencies; or<br><br>(E) Communicating information about a health IT developer's failure to comply with a Condition of Certification, or with any other requirement of this part, to ONC or an ONC-ACB.<br><br>(ii) *Permitted prohibitions and restrictions.* For communications about one or more of the subject matters enumerated in paragraph (a)(1) of this section that is not entitled to unqualified protection under paragraph (a)(2)(i) of this section, a health IT developer may prohibit or restrict communications only as expressly permitted by paragraphs (a)(2)(ii)(A) through (F) of this section.<br><br>(A) *Developer employees and contractors*. A health IT developer may prohibit or restrict the communications of the developer's employees or contractors.<br><br>(B) *Non-user-facing aspects of health IT*. A health IT developer may prohibit or restrict communications that disclose information about non-user-facing aspects of the developer's health IT.<br><br>(C) *Intellectual property.* A health IT developer may prohibit or restrict communications that would infringe the intellectual property rights existing in the developer's health IT (including third-party rights), provided that—<br><br>(1) A health IT developer does not prohibit or restrict, or purport to prohibit or restrict, communications that would be a fair use of a copyright work; and | (D) Communicating information about information blocking and other unlawful practices to government agencies; or<br><br>(E) Communicating information about a health IT developer's failure to comply with a Condition of Certification, or with any other requirement of this part, to ONC or an ONC-ACB.<br><br>Any person who makes a communication covered by (2)(i) to an appropriate entity must not be subject to retaliatory action which could reasonably be considered due to their whistleblowing activity.<br><br>(ii) *Permitted prohibitions and restrictions.* For communications about one or more of the subject matters enumerated in paragraph (a)(1) of this section that is not entitled to unqualified protection under paragraph (a)(2)(i) of this section, a health IT developer may prohibit or restrict communications only as expressly permitted by paragraphs (a)(2)(ii)(A) through (F) of this section.<br><br>(A) *Developer employees and contractors*. A health IT developer may prohibit or restrict the communications of the developer's employees or contractors.<br><br>(B) *Non-user-facing aspects of health IT*. A health IT developer may prohibit or restrict communications that disclose information about non-user-facing aspects of the developer's health IT.<br><br>(C) *Intellectual property.* A health IT developer may prohibit or restrict communications that would infringe the intellectual property rights existing in the developer's | (D) Communicating information about information blocking and other unlawful practices to government agencies; or<br><br>(E) Communicating information about a health IT developer's failure to comply with a Condition of Certification, or with any other requirement of this part, to ONC or an ONC-ACB.<br><br>Any person who makes a communication covered by (2)(i) to an appropriate entity must not be subject to retaliatory action which could reasonably be considered due to their whistleblowing activity.<br><br>(ii) *Permitted prohibitions and restrictions.* For communications about one or more of the subject matters enumerated in paragraph (a)(1) of this section that is not entitled to unqualified protection under paragraph (a)(2)(i) of this section, a health IT developer may prohibit or restrict communications only as expressly permitted by paragraphs (a)(2)(ii)(A) through (F) of this section.<br><br>(A) *Developer employees and contractors*. A health IT developer may prohibit or restrict the communications of the developer's employees or contractors.<br><br>(B) *Non-user-facing aspects of health IT*. A health IT developer may prohibit or restrict communications that disclose information about non-user-facing aspects of the developer's health IT.<br><br>(C) *Intellectual property.* A health IT developer may prohibit or restrict communications that would infringe the intellectual property rights existing in the developer's |

| | | |
|---|---|---|
| (2) A health IT developer does not prohibit the communication of screenshots of the developer's health IT, subject to the limited restrictions described in paragraph (a)(2)(ii)(D) of this section.<br><br>(D) *Screenshots*. A health IT developer may require persons who communicate screenshots to—<br><br>(1) Not alter screenshots, except to annotate the screenshot, resize it, or to redact the screenshot in accordance with § 170.403(a)(2)(ii)(D)(3) or to conceal protected health information;<br><br>(2) Not infringe the intellectual property rights of any third parties, provided that —<br><br>(i) The developer has used all reasonable endeavors to secure a license (including the right to sublicense) in respect to the use of the third-party rights by communicators for purposes of the communications protected by this Condition of Certification;<br>(ii) The developer does not prohibit or restrict, or purport to prohibit or restrict, communications that would be a fair use of a copyright work;<br>(iii) The developer has put all potential communicators on sufficient written notice of each aspect of its screen display that contains third-party content that cannot be communicated because the reproduction would infringe the third-party's intellectual property rights; and<br>(iv) Communicators are permitted to communicate screenshots that have been | health IT (including third-party rights), provided that—<br><br>(1) A health IT developer does not prohibit or restrict, or purport to prohibit or restrict, communications that would be a fair use of a copyright work; and<br><br>(2) A health IT developer does not prohibit the fair use communication of screenshots of the developer's health IT, subject to the limited restrictions described in paragraph (a)(2)(ii)(D) of this section, and with the understanding that any actor disclosing the screenshots are responsible for ensuring that each use is being put to "fair use."<br><br>(D) *Screenshots*. A health IT developer may require persons who communicate screenshots to—<br><br>(1) Not alter screenshots, except to annotate the screenshot, resize it, or to redact the screenshot in accordance with § 170.403(a)(2)(ii)(D)(3) or to conceal protected health information;<br><br>(2) Not infringe the intellectual property rights of any third parties, provided that —<br><br>(i) The developer has used all reasonable endeavors to secure a license (including the right to sublicense) in respect to the use of the third-party rights by communicators for purposes of the communications protected by this Condition of Certification;<br>(ii) The developer does not prohibit or restrict, or purport to prohibit or restrict, communications that would be a fair use of a copyright work; | health IT (including third-party rights), provided that—<br><br>(1) A health IT developer does not prohibit or restrict, or purport to prohibit or restrict, communications that would be a fair use of a copyright work; and<br><br>(2) A health IT developer does not prohibit the fair use communication of screenshots of the developer's health IT, subject to the limited restrictions described in paragraph (a)(2)(ii)(D) of this section, and with the understanding that any actor disclosing the screenshots are responsible for ensuring that each use is being put to "fair use."<br><br>(D) *Screenshots*. A health IT developer may require persons who communicate screenshots to—<br><br>(1) Not alter screenshots, except to annotate the screenshot, resize it, or to redact the screenshot in accordance with § 170.403(a)(2)(ii)(D)(3) or to conceal protected health information;<br><br>(2) Not infringe the intellectual property rights of any third parties, provided that —<br><br>(i) The developer has used all reasonable endeavors to secure a license (including the right to sublicense) in respect to the use of the third-party rights by communicators for purposes of the communications protected by this Condition of Certification;<br>(ii) The developer does not prohibit or restrict, or purport to prohibit or restrict, communications that would be a fair use of a copyright work; |

| | | |
|---|---|---|
| redacted to not disclose third-party content; and<br><br>(3) Redact protected health information, unless the individual has provided all necessary consents or authorizations or the communicator is otherwise authorized, permitted, or required by law to disclose the protected health information.<br><br>(E) Pre-market testing and development. A health IT developer may prohibit or restrict communications that disclose information or knowledge solely acquired in the course of participating in pre-market product development and testing activities carried out for the benefit of the developer or for the joint benefit of the developer and communicator. A developer must not, once the subject health IT is released or marketed for purposes other than product development and testing, and subject to the permitted prohibitions and restrictions described in paragraph (a)(2)(ii) of this section, prohibit or restrict communications about matters enumerated in paragraph (a)(1) of this section.<br><br>(b) *Maintenance of Certification*<br><br>(1) Notice. Health IT developers must issue a written notice to all customers and those with which it has agreements containing provisions that contravene paragraph (a) of this section:<br><br>(i) Within six months of the effective date of the final rule that any communication or contract provision that contravenes paragraph (a) of this section will not be enforced by the health IT developer. | (iii) The developer has put all potential communicators on sufficient written notice of a list of third-party content included in the health IT that cannot be communicated because the reproduction would infringe the third-party's intellectual property rights; and<br>(iv) Communicators are permitted to communicate screenshots that have been redacted to not disclose third-party content; and<br><br>(3) Redact protected health information, unless the individual has provided all necessary consents or authorizations or the communicator is otherwise authorized, permitted, or required by law to disclose the protected health information.<br><br>(E) Pre-market testing and development. A health IT developer may prohibit or restrict communications that disclose information or knowledge solely acquired in the course of participating in pre-market product development and testing activities carried out for the benefit of the developer or for the joint benefit of the developer and communicator. A developer must not, once the subject health IT is released or marketed for purposes other than product development and testing, and subject to the permitted prohibitions and restrictions described in paragraph (a)(2)(ii) of this section, prohibit or restrict communications about matters enumerated in paragraph (a)(1) of this section.<br><br>(3) Unprotected Communications. Specific communications are not extended the protections or restrictions in this section, where those communications are | (iii) The developer has put all potential communicators on sufficient written notice of a list of third-party content included in the health IT ~~each aspect of its screen display that contains third-party content~~ that cannot be communicated because the reproduction would infringe the third-party's intellectual property rights; and<br>(iv) Communicators are permitted to communicate screenshots that have been redacted to not disclose third-party content; and<br><br>(3) Redact protected health information, unless the individual has provided all necessary consents or authorizations or the communicator is otherwise authorized, permitted, or required by law to disclose the protected health information.<br><br>(E) Pre-market testing and development. A health IT developer may prohibit or restrict communications that disclose information or knowledge solely acquired in the course of participating in pre-market product development and testing activities carried out for the benefit of the developer or for the joint benefit of the developer and communicator. A developer must not, once the subject health IT is released or marketed for purposes other than product development and testing, and subject to the permitted prohibitions and restrictions described in paragraph (a)(2)(ii) of this section, prohibit or restrict communications about matters enumerated in paragraph (a)(1) of this section.<br><br>(3) Unprotected Communications. Specific communications are not extended the protections or |

| | | |
|---|---|---|
| (ii) Within one year of the final rule, and annually thereafter until paragraph (b)(2)(ii) of this section is fulfilled, that any communication or contract provision that contravenes paragraph (a) of this section will not be enforced by the health IT developer.<br><br>(2) Contracts and agreements.<br><br>(i) A health IT developer must not establish or enforce any contract or agreement that contravenes paragraph (a) of this section.<br><br>(ii) If a health IT developer has a contract or agreement in existence at the time of the effective date of this final rule that contravenes paragraph (a) of this section, then the developer must in a reasonable period of time, but not later than two years from the effective date of this rule, amend the contract or agreement to remove or void the contractual provision that contravenes paragraph (a) of this section. | considered unprotected in that they are either:<br><br>(i) protected by other legislation or regulation; or<br>(ii) false or unlawful.<br><br>(b) *Maintenance of Certification*<br><br>(1) Notice. Health IT developers must issue a written notice to all customers and those with which it has agreements containing provisions that contravene paragraph (a) of this section:<br><br>(i) Within six months of the effective date of the final rule that any communication or contract provision that contravenes paragraph (a) of this section will not be enforced by the health IT developer.<br><br>(ii) Within one year of the final rule, and annually thereafter until paragraph (b)(2)(ii) of this section is fulfilled, that any communication or contract provision that contravenes paragraph (a) of this section will not be enforced by the health IT developer.<br><br>(2) Contracts and agreements.<br><br>(i) A health IT developer must not establish, renew, or enforce any contract or agreement that contravenes paragraph (a) of this section.<br><br>(ii) If a health IT developer has a contract or agreement in existence at the time of the effective date of this final rule that contravenes paragraph (a) of this section, then the developer must in a reasonable period of time, but not later than two years from the effective date of this rule, agree with the relevant | restrictions in this section, where those communications are considered unprotected in that they are either:<br><br>(i) protected by other legislation or regulation; or<br>(ii) false or unlawful.<br><br>(b) *Maintenance of Certification*<br><br>(1) Notice. Health IT developers must issue a written notice to all customers and those with which it has agreements containing provisions that contravene paragraph (a) of this section:<br><br>(i) Within six months of the effective date of the final rule that any communication or contract provision that contravenes paragraph (a) of this section will not be enforced by the health IT developer.<br><br>(ii) Within one year of the final rule, and annually thereafter until paragraph (b)(2)(ii) of this section is fulfilled, that any communication or contract provision that contravenes paragraph (a) of this section will not be enforced by the health IT developer.<br><br>(2) Contracts and agreements.<br><br>(i) A health IT developer must not establish, renew, or enforce any contract or agreement that contravenes paragraph (a) of this section.<br><br>(ii) If a health IT developer has a contract or agreement in existence at the time of the effective date of this final rule that contravenes paragraph (a) of this section, then the developer must in a reasonable period of time, but not later than two years |

| | | |
|---|---|---|
| | client on a plan to amend the contract or an agreement to remove or void the contractual provision that contravenes paragraph (a) of this section.<br><br>(iii) The plan required by paragraph (ii) of this section must be completed within five years of the effective date of this rule. | from the effective date of this rule,~~amend the contract or~~ agree with the relevant client on a plan to amend the contract or an agreement to remove or void the contractual provision that contravenes paragraph (a) of this section.<br><br>(iii) The plan required by paragraph (ii) of this section must be completed within five years of the effective date of this rule. |

## 21. 170.580 ONC Review of Certified Health IT or a Health IT Developer's Actions

The Task Force was concerned with the idea that direct review communications could be serious in consequence. Specifically, relying on email could be problematic if the respondent is on vacation, out of office, or had left the company.

Recommendation 57

| ORIGINAL | RECOMMENDED REGULATION | COMPARISON / MARKUP |
|---|---|---|
| § 170.505 Correspondence.<br>(a) Correspondence and communication with ONC or the National Coordinator shall be conducted by email, unless otherwise necessary or specified. The official date of receipt of any email between ONC or the National Coordinator and an applicant for ONC-ACB status, an applicant for ONC-ATL status, an ONC-ACB, an ONC-ATL, health IT developer, or a party to any proceeding under this subpart is the date on which the email was sent.<br>(b) In circumstances where it is necessary for an applicant for ONC-ACB status, an applicant for ONC-ATL status, an ONC-ACB, an ONC-ATL, health IT developer, or a party to any proceeding under this subpart to correspond or communicate with ONC or the National Coordinator by regular, express, or certified mail, the | § 170.505 Correspondence.<br>(a) Correspondence and communication with ONC or the National Coordinator shall be conducted by email, unless otherwise necessary or specified. The official date of receipt of any email between ONC or the National Coordinator and an applicant for ONC-ACB status, an applicant for ONC-ATL status, an ONC-ACB, an ONC-ATL, health IT developer, or a party to any proceeding under this subpart is the date on which the email was sent.<br>(b) In circumstances where it is necessary for an applicant for ONC-ACB status, an applicant for ONC-ATL status, an ONC-ACB, an ONC-ATL, health IT developer, or a party to any proceeding under this subpart to correspond or communicate with ONC or the National Coordinator by regular, express, or certified mail, the | § 170.505 Correspondence.<br>(a) Correspondence and communication with ONC or the National Coordinator shall be conducted by email, unless otherwise necessary or specified. The official date of receipt of any email between ONC or the National Coordinator and an applicant for ONC-ACB status, an applicant for ONC-ATL status, an ONC-ACB, an ONC-ATL, health IT developer, or a party to any proceeding under this subpart is the date on which the email was sent.<br>(b) In circumstances where it is necessary for an applicant for ONC-ACB status, an applicant for ONC-ATL status, an ONC-ACB, an ONC-ATL, health IT developer, or a party to any proceeding under this subpart to correspond or communicate with ONC or the National Coordinator by regular, express, or certified mail, the |

| | | |
|---|---|---|
| official date of receipt for all parties will be the date of the delivery confirmation to the address on record. | official date of receipt for all parties will be the date of the delivery confirmation to the address on record.<br>(c) Notices initiating direct review, of potential non-conformity, of non-conformity, of suspension, of proposed termination, of termination, of ban, or concerning the appeals process will be issued simultaneously via certified mail and email. | official date of receipt for all parties will be the date of the delivery confirmation to the address on record.<br>(c) Notices initiating direct review, of potential non-conformity, of non-conformity, of suspension, of proposed termination, of termination, of ban, or concerning the appeals process will be issued simultaneously via certified mail and email. |

The Task Force recommends that ONC clarify in preamble that ONC should use both email and certified mail for notices of initiating direct review, potential non-conformity, non-conformity, suspension, proposed termination, termination and ban. Notices regarding appeals would be the same.

## 22. 170.581 Certification Ban

The sense of the Task Force was that knowledge of past bans was important for stakeholders and therefore indefinite communication of past records (ban with start and end date, if lifted) seems appropriate.

Recommendation 58

Indefinite communication of past records (ban with start and end date, if lifted) seems appropriate.

Recommendation 59

We do not recommend establishing a minimum time period over which a ban must last, even if the health IT developer is a repeat offender. The sense of the Task Force was that a minimum ban time period could have unintended consequences.

## 23. Request for Comment on Application of Conditions and Maintenance of Certification to Self-Developers

The provisions of information blocking and the Assurances Condition of Certification would apply to self-developers also. Most of the provisions of the Communications Condition of Certification would also apply to self-developers. The Task Force identified one area that would require modification for self-developers, which was in (a)(2)(ii)(A) where the Task Force noticed that employees of a developer can have their communications restricted, but that this could

have the consequence of limiting communications of users of the self-developed health IT for the reasons identified under Cures.

Recommendation 60

The Task Force recommends that ONC call out an exception to (a)(2)(ii)(A) for self-developed systems, so that communications by health IT users aren't restricted by being employees of the same company doing the development.

| ORIGINAL | RECOMMENDED REGULATION | COMPARISON / MARKUP |
|---|---|---|
| § 170.403 Communications.<br>(a)(2)(ii)(A) *Developer employees and contractors*. A health IT developer may prohibit or restrict the communications of the developer's employees or contractors. | § 170.403 Communications.<br>(a)(2)(ii)(A) *Developer employees and contractors*. A health IT developer may prohibit or restrict the communications of the developer's employees or contractors. Healthcare organizations self-developing certified systems are not permitted to restrict the communications of their user employees with respect to these provisions. | § 170.403 Communications.<br>(a)(2)(ii)(A) *Developer employees and contractors*. A health IT developer may prohibit or restrict the communications of the developer's employees or contractors. Healthcare organizations self-developing certified systems are not permitted to restrict the communications of their user employees with respect to these provisions. |

[END OF DOCUMENT]