Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing (HTI-1) Final Rule
Information, Resources & Quick Links – January 2024

The Office of the National Coordinator for Health Information Technology (ONC) is the principal federal entity charged with coordinating nationwide efforts to implement and use advanced health IT and to facilitate the electronic exchange of health information. In December, ONC released a final rule – Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing – referred to as "HTI-1" or the "HTI-1 final rule." You can find the final rule here, and the Department of Health and Human Services' (HHS) press release here. Additionally, CHIME's comment letter on the proposed HTI-1 rule can be found here.

For more information on specific topics within the final rule, there are several fact sheets from ONC that are available here. You can sign up for ONC's upcoming information sessions beginning early 2024 to learn more about the final rule. Additionally, you can rewatch and download the slides from each session if you missed them. **As always – you can reach out to us at policy@chimecentral.org with any questions.**

Key Takeaways

This final rule implements the Electronic Health Record (EHR) Reporting Program provision of the 21st Century Cures Act by establishing new Conditions and Maintenance of Certification requirements for health information technology (health IT) developers under the ONC Health IT Certification Program (Program). Additionally, it makes several updates to certification criteria and standards recognized by the Program. The Program updates include revised certification criteria for "decision support interventions," "patient demographics and observations," and "electronic case reporting," as well as a new baseline version of the United States Core Data for Interoperability (USCDI) standard to Version 3.

Additionally, the final rule provides enhancements to support information sharing under the information blocking regulations. According to ONC, the implementation of these provisions will advance interoperability, improve algorithm transparency, and support the access, exchange, and use of electronic health information (EHI). ONC also states that the final rule updates numerous technical standards in the Program in "additional ways to advance interoperability, enhance health IT certification, and reduce burden and costs for health IT developers and users of health IT."

Finally, this final rule continues to implement the provisions of the Cures Act to "improve information sharing", and address information blocking, by providing refined definitions of statutory terms and further identifying practices that are reasonable and necessary and thus, are not considered "information blocking."

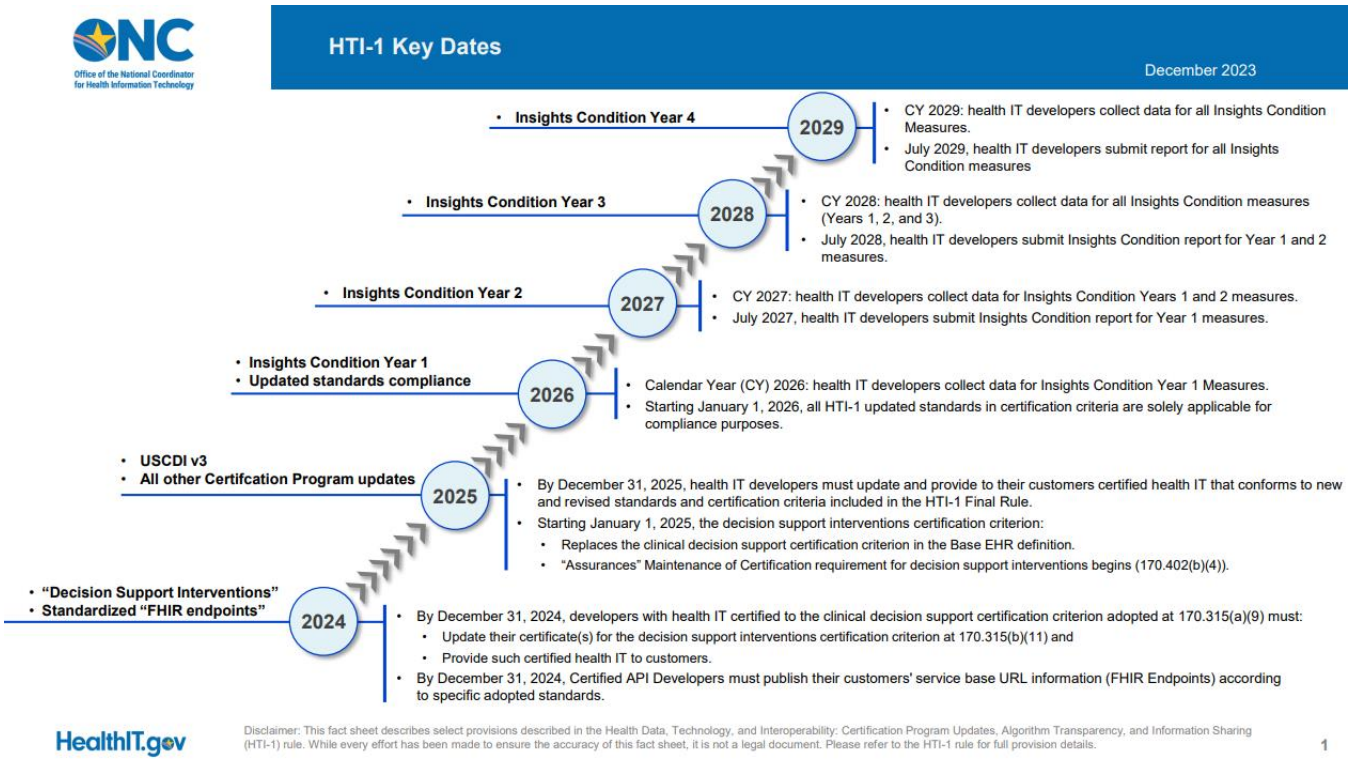
The HTI-1 final rule is consistent with the priorities in several Executive Orders (E.O.), including Executive Order (E.O.) 13985, which aims to "advance health equity, support patient access, improve regulatory transparency and efficiency, advance interoperability, and support the access, exchange, and use of electronic health information (EHI)."

Detailed Summary

ONC Health IT Certification Program Updates – New & Revised Standards and Certification Criteria

This final rule adopts new and revised standards and requirements for the certification of health IT under the Program. Key provisions of this final rule implement the EHR Reporting Program through new Conditions and Maintenance of Certification requirements (referred to as the Insights Condition) for developers of certified health IT, which will "provide transparency into the use and benefits of certified health IT, with an initial focus on interoperability." Additionally, it revises several Program certification criteria, including criteria related to decision support, electronic case reporting, and standards-based application programming interfaces (APIs), as well as raises the baseline version of the United States Core Data for Interoperability (USCDI) from Version 1 to Version 3.

HTI-1 Key Dates



1

Discontinuing Year-Themed "Editions"

ONC has authority[2] to establish a certification program or programs for the voluntary certification of health IT – and first introduced the concept of an "edition" of ONC health IT certification criteria in 2012. ONC no longer believes that it is helpful or necessary to maintain an "edition" naming convention or to adopt entirely new editions of certification criteria to encapsulate updates over time. ONC has finalized their proposed approach to discontinue the use of year-themed editions for ONC Certification Criteria

[1] *ONC HTI-1 Timeline Fact Sheet*. (2023, December). The Office of the National Coordinator for Health IT. https://www.healthit.gov/sites/default/files/page/2023-12/HTI-Timeline-Fact-Sheet_508.pdf.

[2] Section 3001(c)(5) of the PHSA

for Health IT. As proposed – and now finalized – there will be a single set of certification criteria, which will be updated in an incremental fashion in closer alignment to standards development cycles and regular health IT development timelines. In finalizing their policy, all criteria within the Program will be renamed simply as "ONC Certification Criteria for Health IT." Additionally, ONC plans to issue "clear guidance and timelines for when updates would be required."

The United States Core Data for Interoperability Version 3 (USCDI v3) & C-CDA Companion Guide Updates

To meet ONC's statutory responsibilities to improve the standardization of health information that is accessed, exchanged, and used within certified health IT, the final rule adopts the United States Core Data for Interoperability Version 3 (USCDI v3) as a new baseline. ONC has extended the date USCDI v1 expires as a standard for use in the Program to January 1, 2026. In other words, ONC is finalizing USCDI v3 as a new baseline, which would coexist with existing requirements for USCDI Version 1 (v1) until it expires on January 1, 2026 (i.e., USCDI v3 would be the new data set baseline across applicable certification criteria, replacing v1 by Jan. 1, 2026).

ONC is also proposing to adopt the Consolidated Clinical Document Architecture (C-CDA) Companion Guide Release 4.1, and Fast Health Interoperability Resources (FHIR) US Core IG 6.0.1, which would coexist with existing standards until January 1, 2026. A Health IT Module certified to under the Program may support the data elements according to the USCDI v3 standard earlier, if they choose to do so, as soon as the effective date of this final rule, which is February 8, 2024. On and after January 1, 2026, certified Health IT Modules must support those listed data elements according to the USCDI v3 standard.

ONC states that adopting the C-CDA Companion Guide R4.1 is necessary for developers of certified health IT to have appropriate implementation guidance to meet the criteria adopted in this final rule that reference USCDI v3. Additionally, adopting FHIR US Core 6.1.0 establishes a consistent baseline across all Health IT Modules certified to criteria that reference the USCDI and provides clarity to developers of certified health IT regarding which version of the US Core IG they are expected to use in support of USCDI v3 and which version they can expect to encounter when interacting with other actors in the health IT ecosystem, industry-wide.

Requirement for Health IT Developers to Update their Previously Certified Health IT

ONC encourages developers of certified health IT to provide updated Health IT Modules to their customers – and support them in their implementation of such updated modules – in the manner most appropriate to support safety, security and interoperability across settings and systems. That is, the updated Health IT Module is either provided to customers (respective of customer choice) by the timeline established, or it is not.

Further and accordingly, ONC has also finalized that a health IT developer must update a Health IT Module as described and provide customers with updated Health IT Modules in order to maintain certification of the Health IT Module. Consistent with the definition of interoperability and the Assurances Condition and Maintenance requirements, the certified Health IT Module must be able to support all the capabilities to which it is certified, and such capabilities must be provided to the customer for use without special effort by the end of the regulatory specified timelines.

ONC has finalized[3] for each applicable standard, as proposed, that a Health IT Module may be certified to either the existing certification criterion or the revised certification criterion until the end of the transition period when the prior standard(s) and/or certification criterion no longer meet certification requirements. During this time period, existing customers may continue to use the certified health IT they have available to them, and can work with their developers to implement updates in a manner that best meets their needs consistent with the established regulatory timeframes.

Finally, as with the 2015 Edition Cures Update, in order to support effective communication of the updates, ONC will implement a practical approach to facilitate transparency using the Certified Health IT Product List (CHPL) which is the tool that healthcare providers and the general public may use to identify the specific certification status of a certified health IT product at any given time, to explore any certification actions for a product, and to obtain a CMS Certification ID for a product, which is used when participating in some CMS programs.

Decision Support Interventions and Predictive Models

The final rule is significant as it acknowledges and addresses the evolution and expansion of health IT implementation and technology resources in supporting clinical decision-making. The initially adopted[4] Clinical Decision Support (CDS) criterion has witnessed advancements as predictive models play a growing role in informing various decision-makers in healthcare, including clinicians, payers, researchers, and individuals. Health IT Modules, integral to these predictive models, not only provide data for algorithm development but also serve as "the vehicle to influence day-to-day decision-making." Thus, this final rule recognizes the expanding role of Health IT Modules in facilitating the integration and deployment of predictive models within the healthcare ecosystem.

Both structured and unstructured data generated by, and subsequently made available through, certified Health IT Modules power the training and real-world use of predictive models. Developers of certified health IT also create and deploy predictive algorithms or models for use in production environments through their Health IT Modules and, increasingly, such developers also enable other parties, including third-party developers and the developer of certified health IT's customers, to create and deploy predictive models through the developer's Health IT Modules. In turn, certified Health IT Modules are often the vehicle or delivery mechanism for predictive model outputs to reach users, such as clinicians, through clinical decision support.

HHS has a longstanding interest in understanding and addressing concerns about negative, adverse, or harmful consequences that may result from the use of digital data or information about individuals' health (including data analytics), including historically, their use in computerized decision-making. Therefore, ONC had proposed[5] to incorporate new requirements into the Program for Health IT Modules that support the execution of Artificial Intelligence or machine learning-based technology (AI/ML) in support of decision-making as part of the revised CDS criterion.[6] These requirements align with the Biden administration's ongoing efforts "to promote trustworthy AI and the Department's stated policies on advancing equity in the delivery of health and human services."

[3] § 170.315 for all revised certification criteria and in 45 CFR part 170 subpart B
[4] § 170.315(a)(9)
[5] 88 FR 23774–23811
[6] § 170.315(b)(11)

ONC believes that the continued evolution of decision support software, especially as it relates to AI or machine learning-driven "Predictive Decision Support Interventions (Predictive DSIs)", necessitates regulation. ONC therefore proposed requirements for new sets of information that are necessary to guide decision-making based on outputs (e.g., recommendations) from Predictive DSIs, such as an expanded set of "source attributes" and information related to how risk is managed by developers of certified health IT.[7] ONC states that these new sets of information will provide appropriate information to help guide decisions at the time and place of care. In other words, the "Decision Support Interventions" certification criterion has been updated and adopted as a replacement to the current criterion for CDS. This updated certification criterion includes new technical capabilities and transparency requirements for Health IT Modules, "in order to improve trustworthiness and support consistency around the use of predictive algorithms or models in healthcare."

Some commenters – including CHIME – urged ONC to be mindful that "regulations on AI should not stifle innovation or have a chilling effect on beneficial uses of this emerging tool, and that [they] should seek to balance the risks and benefits to consumers of the public availability of information […] and limit adverse effects from a clinical standpoint." ONC responded to these comments that they "are also mindful of the need to balance prescriptiveness and flexibility in [their] requirements for developers of certified health IT with Health IT Modules" and have made several modifications to their proposals "to achieve this balance."

After considering the public comments received, along with both the authorities granted by Congress and directives established by several E.O.s, ONC has finalized most of their proposed changes to the current Program certification criteria. However, they have made modifications "intended to align and simplify technical requirements between evidence-based DSIs and Predictive DSIs." Additionally, there are clarifications to: 1) the definition of Predictive DSI[8]; 2) the scope of technologies considered to be an evidence-based DSI for purposes of the Program; and 3) the scope of source attribute information that must be accessible to users.

ONC has adopted a new definition for Predictive DSI as follows: **"Predictive decision support intervention or Predictive DSI means technology that supports decision-making based on algorithms or models that derive relationships from training data and then produce an output that results in prediction, classification, recommendation, evaluation, or analysis.**"

ONC notes that this version of the definition is not markedly different from the definition they proposed, but they "intend it to be more exacting." Therefore, the examples and discussion regarding scope in the HTI-1 Proposed Rule remain relevant to this definition.[9] Additionally, ONC has clarified the scope of "evidence-based DSIs," as being "limited to only those DSIs that are actively presented to users in clinical workflow to enhance, inform, or influence decision-making related to the care a patient receives and that do not meet the definition for Predictive DSI."

To assist stakeholders in understanding the scope of technologies included in the definition of Predictive DSI, ONC reiterates the following: "The development process whereby models under this definition "learn" relationships in training data and then are used to generate an unknown label or value

[7] 88 FR 23775
[8] § 170.102
[9] 88 FR 23784–23786

(via prediction, classification, recommendation, evaluation, or analysis) that is based on the "learned" relationships is a fundamental differentiator from evidence-based DSIs."

If a technology is used to make "general system improvements" based on training data that consists of "user behavior," it may meet the new definition of a Predictive DSI,[10] if it derived relationships (e.g., correlations) from that training data and then produced an output that results in prediction, classification, recommendation, evaluation, or analysis used to support decision-making. "General system improvements" based on other analysis, such as tracking the time required to perform a task, would likely not meet the definition because that technology does not "derive relationships." According to the final rule, if "general system improvements learned from user behavior," were the outputs of the technology or the effect of the technology, but that output was not used to support decision-making or was not a prediction, classification, recommendation, evaluation or analysis, then this technology likely would not meet [the] finalized definition of Predictive DSI.

ONC has removed "enabled or interfaced with" and replaced it with "supplied by." The final rule's "scope places the knowledge, decision, and ongoing compliance associated with including a Predictive DSI solely within the control of a developer of certified health IT." ONC states that, although "the use of "supplied by" is a different configuration nexus than the proposed attestation statement that used "enables or interfaces with," this approach similarly addresses their intent to only apply additional Predictive DSI related stewardship responsibilities to health IT developers who supply Predictive DSIs as part of their Health IT Module.

With regards to the definition of Predictive DSI, ONC did not propose and has not finalized a definition that is dependent on the entity or party developing the Predictive DSI. In other words, "who develops" a Predictive DSI is separate and distinct from how ONC defines what a Predictive DSI is for the purpose of this regulation. ONC states that while healthcare providers may develop Predictive DSIs (as they have newly defined), they **have not** excluded those provider-authored Predictive DSIs from meeting the regulatory definition. However, ONC notes that the definition is only one part of the Program's policy approach to Predictive DSIs. In response to comments that appeared to conflate "the who" and "the what" with respect to the definition, ONC clarifies that a healthcare provider who self-develops a tool that meets their definition of Predictive DSI is not subject to the requirements in § 170.315(b)(11). In other words, ONC's definition of Predictive DSI is broad in scope, use case inclusive, risk independent, and developer agnostic – meaning it includes certified EHR companies, health systems, academic research labs, and consumer technology firms – to provide a few examples.

In other words, while provider-developed predictive DSIs would still meet the definition of a predictive DSI – they are unlikely to be considered "supplied by," such that requirements to provide information on these predictive DSI would not apply. For example, if the customer (healthcare provider) is simply using a Health IT Module (i.e., CEHRT) to deploy a Predictive DSI, the customer is not subject to any of the Certification Program requirements. If a developer supplies a customer-developed Predictive DSI as part of its Health IT Module, the developer of certified health IT is responsible for the source attribute information, risk management practices, and associated requirements.

[10] § 170.102

Additionally, Health IT Modules certified to § 170.315(b)(11) must support the technical capability for source attribute information to be accessed and modified by users as well as the limited contexts in which developers of certified health IT are required to populate those attributes. Specifically, ONC has limited the scope of their transparency requirements for source attribute information to apply to Predictive DSIs that are supplied by the health IT developer as part of its Health IT Module.

ONC believes that `self-developed' tools, which may be developed by informaticians in a health system and then applied to individual patients by clinical users or others without knowledge of the development or evaluation process could benefit from the inclusion of transparency information guiding their use. Their “finalized certification criterion in § 170.315(b)(11) would result in healthcare providers being equipped with the technological capabilities to deliver such transparency through Health IT Modules certified to § 170.315(b)(11).”

ONC does not believe that large language models (LLMs) should be excluded from their definition for Predictive DSI if the LLMs are used to support decision-making, and do not believe that LLMs are complete “black-boxes” about which no information can be made available to users that would be valuable. Additionally, self-supervised learning models would generally be included within the definition of Predictive DSI. ONC notes that while LLMs and other forms of generative AI often use a combination of unsupervised, self- supervised, supervised and reinforcement learning, and those that include a component of supervised learning, including semi-supervised approaches, would likely meet the definition of Predictive DSI. Rather, ONC has declined to include any exclusionary criteria in their definition for Predictive DSI, including exclusions for specific types of organizations that develop the Predictive DSI, exclusions for specific types of technology that may be considered a Predictive DSI, and exclusions for organizations or technology that may be subject to other federal requirements and authorities.

ONC has also declined to limit the scope of their definition to focus on clinical uses. ONC is declining to further limit the scope of the Predictive DSI definition, especially for administrative functions, which would likely benefit from the transparency these requirements would provide. They note that “even appointment scheduling and block scheduling predictive models have been demonstrated to be of insufficient quality, causing harm to patients.” Further, ONC believes that “greater transparency on the quality of these models could have avoided harm to patients by users interpreting predictions more judiciously or choosing not to use the model, or by motivating developers to retrain the models.”

ONC believes that the source attribute and risk management-related requirements in this rule could help to decrease the likelihood that a model is inappropriately deployed in a Health IT Module in a way that exacerbates bias or poses other risks. **ONC notes that they have finalized a fundamentally limited scope to focus on transparency capabilities and instances where Predictive DSIs (such as LLMs or other generative AI) “are supplied by a developer of certified health IT – and not generally on LLMs or generative AI that may be used in the healthcare ecosystem.”**

ONC has declined to include any exclusionary criteria in their definition for Predictive DSI, including exclusions for specific types of organizations that develop the Predictive DSI, exclusions for specific types of technology that may be considered a Predictive DSI, and exclusions for organizations or technology that may be subject to other federal requirements and authorities.

ONC has declined to respond to commenters' requests to have ONC assess whether specific algorithms, models, and technologies would meet the definition for Predictive DSI. Rather than make specific assessments ONC provides a list of examples of technologies that would likely meet their definition for Predictive DSI – and examples of technologies that would likely not meet their definition for Predictive DSI, the entire list can be found on pages 204-206 of the final rule. Examples include:

- Models that pre-selected or highlighted a default order from an order set based on relationships in training data indicating that order was most likely to be selected **would likely** be considered Predictive DSIs;
- Indices and classification systems developed by expert consensus rather than in empirical data, such as the SOFA index and NYHA Heart Failure classification, **would likely not be** considered Predictive DSIs but **are likely evidence-based DSI** because the score is based on pre-defined rules and not relationships learned in training data;
- Models that generate clinical notes or draft clinical notes and that were trained based on relationships in large data sets of free text, including large language models, and support decision making about what to document in the clinical note, **would likely** be considered Predictive DSIs;
- Models that use natural language processing to route secure messages, which were trained based on the relationship between message contents and the individual who responded to similar messages in the past **would likely** be considered Predictive DSIs; and
- Rules-based algorithms for routing secure messages based on the type of message, rather than relationships in training data, **would likely not** be considered Predictive DSIs.

ONC has finalized that Health IT Modules certified under the Program "must enable a limited set of identified users to select (i.e., activate) evidence-based and Predictive DSIs."[11] Additionally, ONC finalized that Health IT Modules certified must support "source attributes" – categories of technical performance and quality information – for both evidence-based and Predictive DSIs.

Requirements for Decision Support Interventions (DSI) Certification Criterion

The HTI-1 final rule expands the number of source attributes that health IT certified to the DSI criterion must support, including 13 for evidence-based DSIs and 31 source attributes applicable to Predictive DSIs. "Near-term, this set of Predictive DSI source attributes will help create a consistent, industry-wide baseline upon which public-private collaboratives can build as they advance structured "model cards" and other related initiatives." And, "over time, these source attributes will provide the transparency necessary for healthcare organizations and clinical users to better determine whether their Predictive DSIs are fair, appropriate, valid, effective, and safe (FAVES)." Health IT developers will need to update health IT currently certified to the CDS criterion to meet the Predictive DSI criterion's requirements and provide the updated certified health IT to customers by **December 31, 2024**.

Beginning January 1, 2025: 1) developers with health IT certified to the Predictive DSI criterion must comply with the associated maintenance of certification requirement;[12] and 2) the DSI criterion will become the criterion required for healthcare providers to have health IT that continues to meet the Base EHR definition and thus be in a position to have "Certified EHR Technology" for the purposes of certain Centers for Medicare & Medicaid Services programs.

[11] § 170.315(b)(11)(iii)
[12] § 170.402(b)(4)

ONC has finalized their proposals to facilitate the transition from one version of the criterion to the other by updating the 2015 Edition Base EHR definition,[13] which is being replaced with a definition of Base EHR, to include an option for a Health IT Module to meet the definition by either being certified to the existing CDS version of the certification criterion or being certified to the revised DSI criterion for the period up to, and including, December 31, 2024. On and after January 1, 2025, only the DSI criterion will be included in the Base EHR definition and the adoption of the criterion in will expire on January 1, 2025.

Among the numerous standards and certification criteria proposed for revision by the end of 2024, the DSI certification criterion[14] has been prioritized and finalized on the proposed timeline. Based on public comment, ONC has lengthened the implementation timeline "for nearly every other standard and certification criterion proposed in the HTI-1 Proposed Rule, as well as made other timing adjustments that could impact prioritization" for the DSI criterion. ONC believes "these final rule updates will give developers of certified health IT time to focus on implementing the DSI criterion."

The final rule significantly narrows the scope of requirements for Predictive DSI-related source attributes and intervention risk management (IRM) practices, specifically applying them only to Predictive DSIs supplied by the health IT developer as part of its Health IT Module. Additionally, the finalized Top of Form revisions and requirements to the Program's DSI criterion[15] "substantially focus on the responsibilities of developers of certified health IT and the products they bring forward for certification." Specifically, the updated criterion includes new sets of information that ONC believes are necessary to guide decision-making based on outputs (e.g., recommendations) from Predictive DSIs, including:

- An expanded set of "source attributes"[16];
- Requirements for Health IT Modules to enable a limited set of identified users to access complete and up-to-date plain language descriptions of source attribute information
- Requirements for intervention risk management practices to be applied for each Predictive DSI supplied by the health IT developer as part of its Health IT Module; and
- Requirements for summary information related to how intervention risk is managed to be publicly accessible.

ONC notes that Health IT Modules certified to § 170.315(b)(11) must support the technical capability for *other party* source attribute information to be entered into the Health IT Module's source attribute fields, per requirements outlined in the final rule.[17] They state "that if a developer of certified health IT would like to include a capability for *other parties* to record source attributes into a Health IT Module in a way that shields the developer of certified health IT from having access to the *other party* source attributes, they may do so." However, ONC reiterates that "developers of certified health IT are not required to receive, acquire, or otherwise obtain source attribute information for an *other party's* Predictive DSI unless such Predictive DSI is supplied by the developer of certified health IT as part of its Health IT Module."

[13] § 170.102,14
[14] § 170.315(b)(11)
[15] §170.315(b)(11)
[16] § 170.315(b)(11)(iv)
[17] § 170.315(b)(11)(v)(B)

ONC has maintained their description of "*other parties*." As noted in HTI-1 Proposed Rule, *other parties* can include, but are not limited to: a customer of the developer of certified health IT, such as an individual healthcare provider, provider group, hospital, health system, academic medical center, or integrated delivery network; a third-party software developer, such as those that publish or sell medical content or literature used by a DSI; or researchers and data scientists, such as those who develop a model or algorithm that is used by a DSI.[18]

For the purposes of the Program, compliance clarity, and distinguishing a health IT developer's own authored and supplied Predictive DSIs from everyone else, ONC uses the phrase "*other party*," which could include a healthcare provider who self-develops a Predictive DSI. ONC states that "being described as an *other party* imposes no specific regulatory compliance requirement." Further, as noted in HTI-1 Proposed Rule,[19] ONC notes that these "*other parties*" may or may not have a contractual relationship with the developer of certified health IT. Finally, ONC "notes that "*other party*" is a term of art"; and in this final rule, ONC has italicized *other party* and *other parties* to assist readers' understanding that we are using this term of art and not misspelling "another."

In a scenario where an *other party* technology is modified by a different other party (e.g., users or a different third-party developer) such that the initial technology meets the definition of a Predictive DSI, ONC would categorize the modified technology as a Predictive DSI developed by an *other party*. A Health IT Module may be expected to have the technical capability for users to record, change and access source attributes of this modified technology, and may be expected to provide up-to-date source attribute information if the Predictive DSI is supplied by the developer of certified health IT as part of the Health IT Module.

ONC states that they "understand concerns raised by commenters" regarding a potential to create a power imbalance between small and startup "*other parties*" and large incumbent developers of certified health IT, which could either refuse to display source attributes from *other parties* or use information in those source attributes inappropriately – and believes their finalized scope for Predictive DSI source attributes addresses these concerns. Specifically, ONC notes that "these source attributes must be complete and up-to-date if they are supplied by the health IT developer as part of its Health IT Module. In this scenario, *other party* source attributes could be directly supplied to a developer certified health IT's customer who will have both the ability to select this *other party's* Predictive DSI and have a Health IT Module support Predictive DSI source attribute categories for the *other party's* source attributes, even if their developer does not supply a Predictive DSI as part of its Health IT Module," due to newly finalized requirements.[20]

In the final rule, ONC has limited the source attributes that developers of certified health IT with Health IT Modules certified to §170.315(b)(11) are required to complete and keep current to those that are related to Predictive DSIs supplied by the developer of certified health IT – which they believe would limit the resources required to gather information from *other parties*. Health IT Modules must support the capability for *other party* source attribute information to be accessible to users, but developers are not required to receive or proactively acquire such information for user access from these *other parties* just because a user selects (i.e., activates) a Predictive DSI using the developer's Health IT Module.

[18] 88 FR 23796
[19] 88 FR 23796
[20] § 170.315(b)(11)(iii)(B) and § 170.315(b)(11)(iv)(B))

ONC has finalized a different scope with respect to *other party* source attributes, such that developers of certified Health IT are only required to make source attribute information available when the health IT developer supplies the *other party's* Predictive DSI as part of its Health IT Module. The finalized requirements of § 170.315(b)(11) do not extend to developers of certified health IT being accountable for Predictive DSIs developed by their customers or *other party* Predictive DSIs implemented by their customers.

ONC notes that "there is a growing market for DSIs created by *other parties*, which could include third-party businesses or healthcare providers using certified health IT." While they did not finalize proposals to require developers of certified health IT to indicate when source attributes are missing for all *other party*-developed Predictive DSIs, they have finalized that a developer of certified health IT must complete and keep current descriptions of source attribute information as specified[21] for all interventions supplied by the health IT developer, including *other party* interventions the health IT developer supplies as part of its Health IT Module.

ONC believes that this scope appropriately focuses on what a developer of certified health IT can readily and efficiently access in terms of source attribute information. They also finalize that for source attributes,[22] a health IT developer must indicate when information is not available for review. This requirement pertains to both source attributes related to Predictive DSIs authored by the developer of certified health IT and to Predictive DSIs developed by *other parties* that are supplied by the developer as part of its Health IT Module.

Numerous commenters requested that ONC clarify that the certification requirements for developers of certified health IT do not convey an obligation for healthcare providers to review all the source attributes of a DSI each time they choose to use a tool. In response, they state: "Nothing in our proposals nor this final rule would compel a user of certified health IT to review source attributes. However, [they] note it would be a best practice for users to conduct such affirmative reviews in an effort to identify potentially discriminatory tools, as discriminatory outcomes may violate applicable civil rights law."

Further, ONC states that in many cases, developers of certified health IT serve as HIPAA business associates to their covered entity customers, such as healthcare providers or health plans. If an individual requests access to their health information from a HIPAA covered entity (e.g., a healthcare provider that transmits health information in electronic form in connection with an HHS adopted standard transaction) that individual, generally, has a right to access medical and health information (protected health information (PHI)) about themselves in one or more designated record sets (DRS) maintained by or for the individual's HIPAA covered entity. The DRS could include underlying data and information used to generate recommendations about an individual's healthcare, such as information about the use of a Predictive DSI in a healthcare decision and source attribute information associated with use of a Predictive DSI in a healthcare decision.

ONC has finalized a requirement that Health IT Modules must be capable of displaying source attributes from *other parties* and for users to be able to modify attributes for those Predictive DSI. "But that is where the finalized requirements stop. With the exception of Predictive DSIs authored by the health IT developer or those it expressly chooses to supply as part of its Health

[21] § 170.402 (b)(4)
[22] § 170.315(b)(11)(iv)(B)(6); (b)(11)(iv)(B)(7)(iii), (iv), and (v); (b)(11)(iv)(B)(8)(ii) and (iv)

IT Module, we have not required health IT developers with Health IT Modules certified to § 170.315(b)(11) to receive, acquire, or otherwise produce source attributes related to *other party* DSIs." ONC encourages those *other parties* to work with their customers to ensure that source attribute information is full and complete, thereby addressing any potentially unfair market dynamics.

If, as part of its Health IT Module, a health IT developer supplies an LLM or other generative AI that meets the definition of Predictive DSI, the finalized policy[23] requires the health IT developer's Health IT Module certified to § 170.315(b)(11) to enable access to complete and up-to-date plain language descriptions of source attribute information related to that Predictive DSI. The finalized policy also requires Health IT Modules certified to § 170.315(b)(11) to, at a minimum, have the technical capability for users and other parties to populate the source attributes[24] themselves.

ONC has not finalized proposed requirements that Health IT Modules clearly indicate when source attributes from *other parties* are unavailable. Rather, ONC has finalized that Health IT Modules certified to § 170.315(b)(11) must enable a limited set of identified users to access complete and up-to-date descriptions of all source attributes related to evidence-based DSIs and Predictive DSIs that are supplied by the developer of certified health IT as part of their Health IT Module.[25] Moreover, ONC has finalized requirements[26] that Health IT Modules certified to § 170.315(b)(11) must enable a limited set of identified users to record and change source attributes listed in the final rule.[27] ONC has not finalized proposed requirements for Health IT Modules to make source attribute information available via direct display, drill down, or link out.

ONC has finalized requirements related to revising source attribute information[28] with modifications; which requires that a Health IT Module must enable a limited set of identified users to record and change source attributes. **In other words, while ONC has not finalized a requirement for presenting source attribute information to users, Health IT Modules are required to enable a limited set of identified users to access complete and up-to-date plain language descriptions of source attribute information.**

This is a modified version of the proposal – combining the "author and revise" and "review" concepts; ONC states that they intend to "clearly convey that individuals can record and change information within the source attributes." ONC has finalized[29] that for Predictive DSIs, the Health IT Module must enable a limited set of identified users to record, change, and access additional source attribute information not specified[30]. **In this final rule, ONC has limited this capability to only Predictive DSI source attributes – rather than the proposed rule where it applied to both evidence-based and Predictive DSIs.**

Additionally, ONC has modified the capability from "author and revise source attributes beyond those listed" to the capability to "record, change, and access additional source attribute information not specified.". They clarify that developers of certified Health IT Modules are not responsible for the content recorded, changed, or accessed by these users. Further, "as technology related to Predictive

[23] § 170.315(b)(11)
[24] § 170.315(b)(11)(iv)
[25] § 170.315(b)(11)(v)(A)
[26] § 170.315(b)(11)(v)(B)
[27] § 170.315(b)(11)(iv)(A) and (B)
[28] § 170.315(b)(11)(v)(B)(1)
[29] § 170.315(b)(11)(v)(B)(2)
[30] § 170.315(b)(11)(iv)(B)

DSIs continues to evolve and as industry consensus matures, [ONC] expects that new information may need to be made available through source attributes for new models." This final rule has set a "consistent, industry-wide baseline set of source attributes on which these groups may wish to build"; ONC has retained a requirement[31] around authoring source attributes in addition to those listed in the final rule.[32] "This capability will help support healthcare providers who wish to stay at pace with industry consensus around transparency and include additional source attribute information using their certified health IT to do so."

The phrase "limited set of identified users" conveys that the capability is not required for all users of the Health IT Module. Rather – that the capability can be constrained to a smaller user-base that are identified to have the privileges necessary to use the capabilities in § 170.315(b)(11), including the capability to record, change, and access source attributes and source attribute information. ONC has provided this flexibility so that any number and configuration of users may record, change, and access source attribute information according to organizational needs. ONC offers this example: "If a client of a developer of certified health IT hosts source attributes for each deployed evidence-based or Predictive DSI centrally, a Health IT Module could include a hyperlink from a dashboard or other user interface to a user at the point-of-care. Additionally, this flexibility could limit record, change, and access privileges to a user who has responsibilities for an organization's procurement and implementation decisions."

ONC acknowledges that they are aware of industry efforts to standardize a format to display information about technology in the form of a "model card" or "nutritional label" for healthcare.[33] Rather than prescribing uniform presentation of this kind of information, ONC has finalized that developers of certified health IT "should work with their customers to determine the best format and structure of source attribute information." ONC notes that the information required here as source attribute information is similar to the "meta-data" described by commenters.

ONC has identified and finalized source that Health IT Modules are required to enable a limited set of identified users to access complete and up-to-date plain language descriptions of source attribute information for Predictive DSIs. There are nine categories in total, with three categories related to use, three categories related to the development process, and three categories related to performance. They are required as follows:

1) Details and output of the intervention, (i.e., Intervention Details) including:
    - Name and contact information for the intervention developer;
    - Funding source of the technical implementation for the intervention(s) development;
    - Description of value that the intervention produces as an output; and
    - Whether the intervention output is a prediction, classification, recommendation, evaluation, analysis, or other type of output.
2) Purpose of the intervention, including:
    - Intended use of the intervention;
    - Intended patient population(s) for the intervention's use;
    - Intended user(s); and

[31] § 170.315(b)(11)(v)(B)(2)
[32] § 170.315(b)(11)(iv)(B)
[33] 88 FR 23794

- Intended decision-making role for which the intervention was designed to be used/for (e.g., informs, augments, replaces clinical management).

3) Cautioned out-of-scope use of the intervention, including:
   - Description of tasks, situations, or populations where a user is cautioned against applying the intervention; and
   - Known risks, inappropriate settings, inappropriate uses, or known limitations.
4) Intervention development details and input features, including at a minimum:
   - Exclusion and inclusion criteria that influenced the training data set;
   - Use of variables[34] as input features;
   - Description of demographic representativeness according to variables[32] including, at a minimum, those used as input features in the intervention;
   - Description of relevance of training data to intended deployed setting.
5) Processes used to ensure fairness in development of the intervention, including:
   - Description of the approach the intervention developer has taken to ensure that the intervention's output is fair; and
   - Description of approaches to manage, reduce, or eliminate bias.
6) External validation process, including:
   - Description of the data source, clinical setting, or environment where an intervention's validity and fairness has been assessed, other than the source of training and testing data;
   - Party that conducted the external testing;
   - Description of demographic representativeness of external data according to variables[32] including, at a minimum, those used as input features in the intervention; and
   - Description of external validation process.
7) Quantitative measures of performance, including:
   - Validity of intervention in test data derived from the same source as the initial training data;
   - Fairness of intervention in test data derived from the same source as the initial training data;
   - Validity of intervention in data external to or from a different source than the initial training data;
   - Fairness of intervention in data external to or from a different source than the initial training data; and
   - References to evaluation of use of the intervention on outcomes, including, bibliographic citations or hyperlinks to evaluations of how well the intervention reduced morbidity, mortality, length of stay, or other outcomes.
8) Ongoing maintenance of intervention implementation and use, including:
   - Description of process and frequency by which the intervention's validity is monitored over time;
   - Validity of intervention in local data;
   - Description of the process and frequency by which the intervention's fairness is monitored over time; and
   - Fairness of intervention in local data.
9) Update and continued validation or fairness assessment schedule, including:
   - Description of process and frequency by which the intervention is updated; and

[34] Paragraph (b)(11)(iv)(A)(5)-(13)

- Description of frequency by which the intervention's performance is corrected when risks related to validity and fairness are identified.

ONC has finalized the following required source attributes specific to evidence-based DSIs: use of patient demographic, use of social determinants of health (SDOH), and use of health status assessment data elements[35] as expressed in the standards in USCDI.[36] ONC notes that compliance with USCDI v1 will be required to initially meet this certification criterion until compliance with USCDI v3 becomes required as part of this certification criterion (i.e., January 1, 2026). As such, the first compliance date associated with § 170.315(b)(11) a Health IT Module may include, but is not required to include, identification of the use of patient demographic data elements that are only found in USCDI v3 as part of evidence-based DSIs.[33] For evidence-based DSIs, Health IT Modules must: 1) enable selection (i.e., activation of); 2) enable users to access source attributes for; and 3) support "feedback loop" functionality for.

ONC believes that the information available as source attributes will have value both as reference information to individual users evaluating the use of a DSI on an individual patient – for example, by assessing whether it has been recently evaluated at their health system and whether it has been shown to perform well for a patient like theirs – and for the organization during procurement, implementation, and analysis.

To further address potential ambiguity about how source attributes must be implemented in Health IT Modules certified to § 170.315(b)(11), ONC has finalized uniform requirements[37] for Health IT Modules to support both evidence-based and Predictive DSI source attributes. This means that all Health IT Modules certified to § 170.315(b)(11) must support the categories, but not necessarily the content, for each source attribute listed. For example, Health IT Modules must support user access to complete and up-to-date source attribute information only if the Predictive DSI is supplied by the health IT developer as part of its Health IT Module. ONC has provided additional specificity about the technical capabilities required to support source attributes.[38] ONC has not finalized their proposal for an attestation statement. Rather, they have finalized[39] a set of four capabilities that Health IT Modules must support related to source attributes.

Missing Source Attributes

While ONC "noted in the HTI-1 Proposed Rule that missing source attribute information would be foundational for users' understanding of the DSI regardless of whether the intervention developer was a developer of certified health IT, a customer of the developer of certified health IT, an academic health system, integrated delivery network, a third-party software developer, or other party[40]," they also acknowledged there may be circumstances where a developer of certified health IT may not have information pertaining to a source attribute for a Health IT Module to enable such user review. In response to public comments received, ONC has made two overall adjustments. First, they did not finalize their original proposals for missing source attributes as it relates to other parties. Rather, they have constrained the overall scope of the certification criterion and the developer of the certified Health IT Module's accountability to those Predictive DSIs supplied by the health IT

[35] § 170.315(b)(11)(iv)(A)(5) through (13)
[36] § 170.213
[37] § 170.315(b)(11)(iv)
[38] § 170.315(b)(11)(v)
[39] § 170.315(b)(11)(v)
[40] 88 FR 23795

developer as part of its Health IT Module. As a result, in circumstances where a developer of certified health IT has not supplied *an other* party's Predictive DSI as part of its Health IT Module the developer is not accountable for the unavailability of those Predictive DSI's source attribute information. Second, ONC has finalized a certification requirement for Health IT Modules to indicate when information is not available for specific source attributes only.

ONC has finalized[41] requirements that for Predictive DSI and, a Health IT Module must indicate when information is not available for review for source attributes.[42] ONC notes that the implication of this finalized policy is twofold: 1) developers of certified health IT with Health IT Modules certified to § 170.315(b)(11) must enable a limited set of identified users to access complete and up-to-date plain language descriptions for nearly all source attributes[43]; and 2) developers of certified health IT with Health IT Modules certified to § 170.315(b)(11) must enable such access for evidence-based and Predictive DSIs at least when those DSIs are supplied by the health IT developer as part of its Health IT Module.

In some limited circumstances, information for specific source attributes related to Predictive DSIs supplied by the health IT developer as part of its Health IT Module may not be available nor re-creatable. ONC states that for example, "health IT developers that supply Predictive DSIs that use models provided through the peer reviewed literature, such as ASCVD, eGFR, APACHE IV, and LACE+ models may not have access to training data that would allow them to: 1) provide a description of demographic representativeness of the training data[44]; 2) generate measures of validity in test data derived from the same source as the initial training data[45]; and 3) generate measures of fairness in test data derived from the same source as the initial training data.[46]

In cases where information is only available through published literature, developers may provide information for these source attributes that indicate that the relevant information is not available and that it cannot be replicated. In these cases, ONC encourages organizations to perform external validation of these models and believes that providing users information on the results of that work will be of high value. ONC notes that where source attribute information is available for Predictive DSIs in these scenarios, or where source attribute information can be extrapolated from the literature (e.g., intended use, cautioned out-of-scope use, or intended population, etc.) source attribute information should be accessible and modifiable consistent with the final rule's requirements.[47]

ONC has "left flexibility to developers of certified health IT and their customers to choose if and how to indicate that information is missing, when they believe doing so is valuable, so that they may avoid pejorative and misleading language." Additionally, as part of this final rule's focus on providing information only for Predictive DSIs supplied in Health IT Modules, ONC declines to require that Health IT Modules display or "denote" when another system includes a third-party model.

Intervention Risk Management (IRM) Requirements for Predictive DSI

[41] § 170.315(b)(11)(v)(A)(2)
[42] §170.315(b)(11)(iv)(B)(6); (b)(11)(iv)(B)(7)(iii), (iv), and (v); (b)(11)(iv)(B)(8)(ii) and (iv); and (b)(11)(iv)(B)(9)
[43] Except those listed in § 170.315(b)(11)(v)(A)(2)
[44] § 170.315(b)(11)(iv)(B)(4)(iii)
[45] §170.315(b)(11)(iv)(B)(7)(i)
[46] § 170.315(b)(11)(iv)(B)(7)(ii)
[47] § 170.315(b)(11)(v)

In response to public comments, ONC has not finalized the requirements described in the HTI-1 Proposed Rule for developers of certified health IT to receive or have access to specific risk management information from *other parties* – except when the health IT developer supplies *an other party* Predictive DSI as part of its Health IT Module. This means there are no expectations that developers review risk management information from other parties with whom they have no relationship and with whom they have not expressly chosen to supply a Predictive DSI as part of their Health IT Module. This also excludes all *other party* Predictive DSIs that their customers choose to implement as well as any Predictive DSIs that their customers author.

ONC has finalized modifications to their proposal for IRM practices,[48] and did not adopt the requirement for detailed documentation originally proposed. The finalized policy requires that IRM practices must be applied for each Predictive DSI supplied by the health IT developer as part of its Health IT Module, which is similar to how ONC described them in the HTI-1 Proposed Rule.[49] ONC had proposed three intervention risk management practices: 1) risk analysis, 2) risk mitigation, and 3) governance.[50]

Overall, ONC identified these as practices that promote transparency regarding how the developer of certified health IT analyzes and mitigates risks at the organization level, including proposals that would have such developers establish policies and implement controls for governance, inclusive of how data are acquired, managed, and used in Predictive DSIs. Together, transparency regarding the technical and performance details of a Predictive DSI, as well as the organizational competencies of the developer of certified health IT to manage risks for a Predictive DSI, were intended to contribute to the trustworthiness of these emerging and important technologies. ONC reiterates that the Program is not predicated on levels of risk and the DSI criterion will continue to be agnostic to specific use cases, intended uses, and risks.

ONC has also finalized[51] that intervention risk management (IRM) practices must be applied for each Predictive DSI supplied by the health IT developer as part of its Health IT Module, "including requirements to subject Predictive DSIs to risk analysis and risk mitigation related to validity, reliability, robustness, fairness, intelligibility, safety, security, and privacy." In other words, as stated in the HTI-1 Proposed Rule[52], ONC will require the developers of certified health IT engage in and document risk management practices related to these eight characteristics. ONC notes that for governance practices, they have finalized[53] requirements for Health IT Modules to be subject to policies and implemented controls for governance, including how data are acquired, managed, and used.

As ONC noted in the HTI-1 Proposed Rule[54], as a consequence of adopting this revised DSI criterion, developers of certified health IT with Health IT Module(s) certified to § 170.315(b)(11) are required to submit real world testing plans and corresponding real world testing results,[55] demonstrating the real world use of each type of DSI – including evidence-based DSIs and Predictive DSIs. This also means that a developer of certified health IT with a Health IT Module certified to § 170.315(b)(11) must apply IRM practices for each Predictive DSI supplied by the health IT developer as described[56] and submit

[48] § 170.315(b)(11)(vi)
[49] 88 FR 23798
[50] 88 FR 23780
[51] § 170.315(b)(11)(vi)
[52] 88 FR 23799
[53] § 170.315(b)(11)(vi)(C)
[54] 88 FR 23783
[55] Consistent with § 170.405
[56] § 170.315(b)(11)(vi)

summary information of their IRM practices to its ONC-ACB via publicly accessible hyperlink[57] before December 31, 2024.

ONC has finalized as part of Governance requirements[58], that for each Predictive DSI supplied by the developer as part of its Health IT Module, the Predictive DSI must be subject to policies and implemented controls for governance, including how data are acquired, managed, and used. ONC clarifies that the expectation as described in the Proposed Rule that developers receive or have access to risk management information for Predictive DSIs developed by *other parties* is generally inapplicable, unless the developer of health IT is the one supplying the *other party's* Predictive DSI as part of its Health IT Module.

ONC notes that developers should implement practices in full awareness that this final rule will not change their responsibility under other applicable laws, including those that provide legal protections to minimize risk practices and prohibit discrimination. They expect that model developers will use data for training and testing consistent with applicable law, patients' expectations, and any patient consent or preference given. Further, ONC declines to further specify practices that would disqualify a developer from the Program, beyond the eight characteristics that must be addressed.

However, ONC states that they "have provided substantial flexibility in the risk management practices developers engage in within those characteristics and the associated documentation. Developers may therefore choose to apply different levels of rigor to the risk analysis, risk mitigation, and governance of different Predictive DSIs." Similarly, developers of certified health IT may choose to apply different levels of detail describing their approaches to risk management practices as part of the summary information that must be summited per the final rule's requirements.[59]

Additionally, ONC notes that, "similar to when a HIPAA covered entity or business associate engages with a cloud service provider a developer of certified health IT, supplying *an other* party-developed Predictive DSI as part of its Health IT Module, should understand the ways in which the technology or solution offered by the *other party* would seek to connect to or integrate with the certified health IT developer's product(s), so that the covered entity (CE) or business associate (BA) can appropriately conduct its own risk analysis and establish risk Associate management policies, as well as enter into appropriate Business Agreements (BAAs).

They provide the example of a "health IT developer providing certified health IT as a business associate may consider including in its risk analysis any risks associated with a decision by a covered entity to connect or integrate *an other* party's Predictive DSI with the developer's certified health IT products". Under the HIPAA Security Rule, business associates have an independent obligation to identify and manage risks, regardless of whether or not a BAA exists. If a business associate relationship exists and a BAA does not exist, the absence of a BAA does not relieve the business associate from HIPAA Security Rule obligations.

ONC notes that this approach also aligns with HIPAA Security Rule requirements for CEs and BAs. HIPAA covered entities, such as healthcare providers and health plans, are generally among the customers of developers of certified health IT. In many cases, developers of certified health IT serve as

[57] § 170.523(f)(1)(xxi)
[58] § 170.315(b)(11)(vi)(C)
[59] § 170.523(f)(1)(xxi)

HIPAA business associates to their covered entity customers, such as healthcare providers or health plans – and therefore, must comply with the HIPAA Security Rule. ONC states that the "HIPAA Security Rule requires covered entities and business associates to identify and assess risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI ("ePHI") when conducting the risk analysis and risk management required by the Security Rule, including any risks of third-party access to a covered entity's or business associate's information systems that contain electronic protected health information."

Additionally, ONC notes that many of the terms and concepts finalized in the IRM requirements rely on the National Institute of Standards and Technology's (NIST) AI Risk Management Framework (RMF). Specifically, the AI RMF's Govern Section 6 discusses a need for policies and procedures to be in place to address AI risks and benefits arising from third-party software and data. ONC notes that while not required to follow the NIST AI RMF, developers of certified health IT may wish to review Govern Section 6 as it provides a number of suggested actions and documentation questions that ONC believes would be informative towards meeting governance requirements.

Similarly, The Office of the Comptroller of Currency described[60] several best practices related to risk management of models developed by third parties, including seventeen specific items included on its internal control questionnaire. Many of these practices could apply to the development of governance processes pertaining to risk management of models authored by other parties including, for example, "When relying on third-party models, does management obtain ongoing performance monitoring and outcomes analysis of the model conducted by third parties."

Assurances Condition and Maintenance of Certification

As a Condition of Certification requirement under the Program, health IT developers are required to provide an assurance that they will not interfere with a customer's timely access to interoperable health IT certified under the Program. This Condition of Certification also includes two accompanying Maintenance of Certification requirements that require health IT developers to update certified Health IT Modules to all applicable revised certification criteria and provide all Health IT Modules certified to a revised certification criterion to its customers of such certified health IT within timeframes established and specified,[61] with a 12-month timeframe for new customers.

Additionally, in consideration of the scope reductions ONC has made to this final certification criterion, they determined that a supportive Maintenance of Certification requirement as part of the Assurances Condition of Certification is necessary to fully implement their policy objectives and proposals. Specifically, ONC has finalized an "Assurances" Maintenance of Certification requirement[62] that starting January 1, 2025, and on an ongoing basis thereafter, health IT developers with Health IT Modules certified under the Program review and update as necessary, source attribute information[63], risk management practices[64], and summary information provided.[65]

[60] *Agencies issue final guidance on Third-Party risk management*. (n.d.). OCC.gov. https://www.occ.gov/news-issuances/news-releases/2023/nr-ia-2023-53.html
[61] Part 170
[62] 45 CFR 170.402(b)(4)
[63] § 170.315(b)(11)(v)(A) and (B)
[64] § 170.315(b)(11)(vi
[65] § 170.523(f)(1)(xxi)

According to ONC, this reinforces a health IT developer's ongoing responsibility to enable users to access complete and up-to-date descriptions of DSI source attribute information to review and update as necessary IRM practices for all Predictive DSIs it supplies as part of its Health IT Module, and to ensure the ongoing public availability of summary IRM practice information as submitted to their ONC-ACB via hyperlink.[66]

ONC notes that they believe these existing requirements within the Assurance Condition pertain to both evidence-based and Predictive DSIs, as well as IRM practices, and this specific additional Maintenance of Certification requirement is necessary because of the unique, evolving, and dynamic nature of DSIs. Moreover, it is "important for users of health IT certified to § 170.315(b)(11) as well as the Secretary [of HHS] to have as an explicit assurance that developers of certified health IT are keeping source attribute information up-to-date and, as applicable, that such developers are committed to IRM practices."

For example, both evidence-based and Predictive DSIs use EHI as key input data in underlying rules and models. Supplying DSIs without accompanying accurate and up-to-date documentation could inhibit the appropriate use of EHI. Without information on the DSI supplied by the developer of certified health IT, users will not be able to adequately determine whether the developer of certified health IT's supplied DSI is fit for their purpose, or whether they should select a more effective DSI.

Insights Condition and Maintenance of Certification

The Cures Act required ONC to establish the EHR Reporting Program – and specified that a health IT developer be required to submit responses to the reporting criteria developed with respect to all certified technology offered by the health IT developer. This final rule created the Insights Condition and Maintenance of Certification ("Insights Condition") within the ONC Health IT Certification Program to provide transparent reporting on certified health IT.

The Insights Condition's reporting intends to: 1) address information gaps in the health IT marketplace; 2) provide insights on the use of specific certified health IT functionalities; and 3) provide information about use of certified functionalities by end users. The HTI-1 final rule adopts seven measures across four areas related to interoperability: individuals' access to EHI, clinical care information exchange, standards adoption and conformance and public health information exchange. Each of the measures have metrics which developers of certified health IT are required to report on. On the HTI-1 Final Rule landing page you can find measure specification sheets and a fact sheet (all also linked to at the end of this Cheat Sheet) which provide further details on the specific metrics associated with the Insights Condition measures.

The finalized Insights Condition requires a health IT developer participating in the ONC Health IT Certification Program to report on a measure if the developer has each of the following:

1) At least 50 hospital sites or 500 individual clinician users across their certified health IT;
2) Any health IT certified to the certification criteria specified in each measure; and
3) Any users using the certified health IT associated with the measure.

Developers of certified health IT who do not meet the qualifications above will submit a response (attestation) to indicate that they do not meet the minimum reporting qualifications for a measure.

[66] § 170.523(f)(1)(xxi)

The reporting period is one calendar year, with 6 months provided for collating the data. Responses will be submitted annually, during the month of July. The measures and metrics are phased in over three years according to the schedule shown in the table below. “Year 1” data collection starts in calendar year (CY) 2026 (January 1, 2026 – December 31, 2026), with response submissions due in July 2027. Reporting is on an annual basis thereafter. “Year 2” measures and related metrics will begin data collection CY 2027, with reporting July 2028 (and annually thereafter). The “Year 3” measures and related metrics start data collection CY 2028, with reporting July 2029 (and annually thereafter).

Information Blocking Updates: Definitions and Exceptions

CHIME has consistently requested additional resources and education from ONC on information blocking. In this final rule, ONC states: “In response to the comment indicating concern for ONC to extend adequate education on information blocking, we note our deliberate focus on developing accessible, user-friendly resources to help inform the effective implementation of these policies. This includes, but is not limited to, Frequently Asked Questions, recorded national webinars, and infographics all accessible on the ONC website.”

Additionally, ONC proposed and has finalized to revise the definition for “information blocking” to remove the time period for which EHI is limited to the data elements represented in the USCDI v1 because, as of Oct. 6, 2022, EHI is no longer limited to the data elements represented in the USCDI v1.

Offer Health Information Technology or “Offer Health IT”
The HTI-1 final rule defines what it means to “offer health IT” for purposes of the information blocking regulations. **This definition confirms that proffering or supplying any certified health IT to be deployed by others will generally be considered an offer of health IT, while confirming that certain implementation and use activities are not considered an offer.** The finalized definition also narrows the potential applicability of the “health IT developer of certified health IT” definition by explicitly excluding certain activities from what it means to “offer” health IT – as detailed below.

Under the information blocking regulatory framework, health IT developers of certified health IT are held to a different standard with respect to information blocking – and are therefore subjected to higher potential financial penalties for information blocking than healthcare providers. A “Health IT developer of certified health IT” is defined for purposes of the information blocking regulations in statute.[67] As ONC discussed in the ONC Cures Act Final Rule,[68] the definition finalized includes offerors of certified health IT who do not themselves develop certified health IT or take responsibility for the health IT’s certification status under the Program. **Specifically, ONC explained that “an individual or entity that offers certified health IT” would include “any individual or entity that under any arrangement makes certified health IT available for purchase or license.”[69]**

The definition's scope, including exclusions, holds significance for healthcare delivery organizations (HDOs), which may function as healthcare provider actors in most scenarios and certified health IT developer actors in specific instances by offering health IT to third parties. This categorization influences the knowledge standard within the information definition and potential liability for information blocking violations. **If subsidizing providers are recognized as certified**

[67] 45 CFR 171.102
[68] 85 FR 25798 through 25799
[69] 85 FR 25798, quoted and cited in the HTI-1 Proposed Rule at 88 FR 23857

health IT developers (as offerors of health IT), they may face additional civil monetary penalties (CMPs) for information blocking under the Cures Act. Alternatively, if subsidizing providers (i.e., "offerors of health IT") are categorized as healthcare provider actors, they could be subject to the proposed HHS disincentives (financial penalties) upon finalization of that proposed rule.

Both individuals or entities that otherwise fall into at least one category of actor as defined[66] such as healthcare providers – and individuals or entities that otherwise would not fit the definition of any category of actor could offer certified health IT that they did not themselves develop or present for certification. As offerors of certified health IT, these individuals or entities could engage in conduct that constitutes information blocking[70], such as through contractual terms or practices undertaken in operating and maintaining health IT deployed by or for another individual or entity.

In the HTI-1 Proposed Rule[71], ONC proposed to codify[66] a definition of what it means to offer certified health IT. As proposed, the definition would provide clarity about the implications under information blocking regulations of making available funding subsidies and certain features or uses of certified health IT as well as engaging in certain other conduct. ONC specifically proposed to define the term "offer health information technology" or "offer health IT." The HTI-1 final rule changes the wording in the "health IT developer of certified health IT" definition so that it remains clear that a healthcare provider that self-develops certified health IT will not be considered a health IT developer of certified health IT if the provider does not "offer" any certified health IT.

The definition proposed for offer health IT generally includes providing, supplying, or holding out for potential provision or supply, certified health IT under any arrangement or terms, but explicitly excludes certain arrangements and activities. ONC proposed exclusions of certain arrangements and activities from the offer health IT definition to serve two primary purposes:

> 1) to encourage certain beneficial arrangements under which providers in need can receive subsidies for the cost of obtaining, maintaining, or upgrading certified health IT; and
> 2) to give healthcare providers (and others) who use certified health IT concrete certainty that implementing certain health IT features and functionalities, as well as engaging in certain practices that are common and beneficial in an EHR-enabled healthcare environment, will not be considered an offering of certified health IT (regardless of who developed that health IT).

ONC believes that wording the offer health IT definition[72] to focus (as proposed[73]) on holding out or providing or supplying under any arrangement certified health IT "for use by" others may be a source of uncertainty for healthcare providers, and for others who deploy Certified API Technology in the role of an API Information Source. This uncertainty could relate to the implications for purposes of the offer health IT definition of a healthcare provider or other individual or entity in the role of an API Information Source making Certified API Technology available to individuals and entities (other than their own employees and contractors) in the role of API User. Therefore, ONC has revised the wording of the finalized "offer health IT" definition in order to improve certainty for individuals and entities who function in the role of an API Information Source[74] or function in an equivalent role where any APIs involved are not certified but may be part of health IT product(s) that also include one or more Health IT Modules certified under the Program.

[70] § 171.103
[71] 88 FR 23858
[72] § 171.102
[73] 88 FR 23915
[74] Defined in § 171.102 by cross-reference to § 170.404(c)

Specifically, ONC has replaced in the finalized offer health IT definition the phrase "for use" with the phrase "for deployment by or for." They state that this wording is more consistent with the distinction between the act of connecting to, interacting with, or otherwise making use of a health IT item or service (e.g., as an API User) and the act of allowing for such connections or interactions with the health IT that an individual or entity (e.g., a healthcare provider) relies on in conducting its own business operations.

Additionally, ONC notes that this updated wording encompasses the full array of models through which individuals and entities obtain health IT for implementation or other deployment in their operations. They include "or for" in this finalized wording to "ensure it is clear that the offer health IT definition is met regardless of whether the customer to whom the health IT is provided or supplied deploys the health IT by themselves or deploys the health IT by having the offeror or any third party(ies) do some or all such implementation and maintenance for them."

As finalized: **"Health IT developer of certified health IT means an individual or entity, other than a healthcare provider that self-develops health IT that is not offered to others, that develops or offers health information technology."**[75]

As finalized: **"Offer health information technology or offer health IT means to hold out for sale, resale, license, or relicense; or to sell, resell, license, relicense, or otherwise provide or supply health information technology**[76] **for deployment by or for other individual(s) or entity(ies) under any arrangement except for certain excluded activities and arrangements."**

The "offer health IT" definition excludes making available funding to obtain or maintain certified health IT, provided the funding is made available without condition(s) limiting the interoperability, or use of the technology to access, exchange or use EHI for any lawful purpose. Second, the finalized "offer health IT" definition also explicitly codifies that healthcare providers or other health IT users do not "offer health IT" when they engage in certain health IT implementation and use activities, regardless of whether they obtain that health IT from a commercial developer or a reseller or develop it themselves.

Activities and arrangements that are considered to be excluded from what it means to offer health IT are described in this final rule. The excluded arrangements and activities that ***would not*** constitute "offer health IT" include:

1) Donation and subsidized supply arrangements are not considered offerings when an individual or entity donates, gives, or otherwise makes available funding to subsidize or fully cover the costs of a healthcare provider's acquisition, augmentation, or upkeep of health IT, provided such individual or entity offers and makes such subsidy without condition(s) limiting the interoperability or use of the technology to access, exchange or use EHI for any lawful purpose.
2) Health IT implementation and use activities conducted by an individual or entity, such as issuing login credentials.

[75] As that term is defined in 42 U.S.C. 300jj(5)), and which has, at the time it engages in a practice that is the subject of an information blocking claim, one or more Health IT Modules certified under a program for the voluntary certification of health information technology that is kept or recognized by the National Coordinator pursuant to 42 U.S.C. 300jj-11(c)(5) (ONC Health IT Certification Program)
[76] As that term is defined in 42 U.S.C. 300jj(5) and where such health information technology includes one or more Health IT Modules certified under the ONC Health IT Certification Program

3) Certain consulting and legal services – including those furnished by outside counsel and Health IT consultant assistance selection, implementation, and use consulting services.
4) Comprehensive and predominantly non-health IT administrative or operations management services—when an individual or entity furnishes a healthcare provider with administrative or operational management consultant services and the consultant acts as the agent of the provider or otherwise acts on behalf of the provider in dealings with one or more health IT developer(s) or vendor(s), or managing the day-to-day operations and administrative duties for the health IT, or both. To be consistent with this subparagraph, such services must be furnished as part of a comprehensive array of predominantly non-health IT administrative and operational functions that would otherwise be executed by the healthcare provider.

Exclusion of Certain Funding Subsidy Arrangements from Offer Health IT Definition

ONC proposed that the donation and subsidized supply arrangements exclusion in the offer health IT definition to encompass arrangements where "an individual or entity donates, gives, or otherwise makes available funding to subsidize or fully cover the costs of a healthcare provider's acquisition, augmentation, or upkeep of health IT."[77] They stated in the HTI-1 Proposed Rule that the proposed donation and subsidized supply arrangements exclusion "would remove from the definition of offer health information technology or offer health IT the provision of subsidies, in the form of funding or cost coverage subsidy arrangements for certified health IT."[78]

The definition's scope, including exclusions, holds significance for healthcare delivery organizations (HDOs), which may function as healthcare provider actors in most scenarios and certified health IT developer actors in specific instances by offering health IT to third parties. This categorization influences the knowledge standard within the information definition and potential liability for information blocking violations. If subsidizing providers are recognized as certified health IT developers (as offerors of health IT), they may face additional civil monetary penalties (CMPs) for information blocking under the Cures Act. Alternatively, if subsidizing providers (i.e., "offerors of health IT") are categorized as healthcare provider actors, they could be subject to the proposed HHS disincentives (financial penalties) upon finalization of that proposed rule.

ONC has finalized the donation and subsidized supply arrangements exclusion of the offer health IT definition as proposed. The donation and subsidized supply arrangements exclusion as proposed and as finalized is conditional, as indicated by language included in the offer health IT definition: "provided such individual or entity offers and makes such subsidy without condition(s) limiting the interoperability or use of the technology to access, exchange, or use electronic health information for any lawful purpose."

Thus, the donation and subsidized supply arrangements exclusion does not apply if the subsidy is conditioned on limiting the interoperability or use of the technology to access, exchange, or use EHI for any lawful purpose. "Any agreement terms, statements (written or oral), patterns of conduct, or singular actions whereby the source of donation or funding subsidy conditions the donation on the recipient's limiting its use of health IT or its access, use, or exchange of EHI in ways specified or signaled by the funding source would be considered a condition limiting interoperability or use of the technology."

[77] 88 FR 23915
[78] 88 FR 23859

Further, ONC states that: "Provision of funding to a recipient who will use it to cover some or all of the recipient's health IT acquisition, augmentation, or upkeep cost is explicitly excluded from the offer health IT definition. Likewise, arrangements whereby a funding source (whether or not referenced or styled as a "donor") pays, remits, or otherwise transfers to a third-party funds covering the cost (in whole or part) of a healthcare provider's acquisition, augmentation, or upkeep of health IT are explicitly excluded from the offer health IT definition to the extent they are consistent with the policies in the "donation and subsidized supply arrangements exclusion."

To prevent any potential confusion or misunderstanding about the significance of ONC's reference to "subsidized supply" arrangements in the text of the exclusion of the offer health IT definition, they note that "this is included to explicitly recognize a type of arrangement whereby a donor or other subsidy source subsidizes or fully covers costs by payment of such costs to the individual or entity that develops or offers the health IT item(s) or service(s) subsidized." Further, the "exclusion in the offer health IT definition explicitly and intentionally limits application of the donation and subsidized supply arrangements exclusion to those arrangements whereby the source of the subsidy makes available funding to cover costs of acquisition, augmentation, or upkeep of health IT."

Additionally, the finalized first exclusion of the definition encompasses furnishing monetary resources[79] – meaning, "subsidies, in the form of funding or cost coverage subsidy arrangements" for an item or service. ONC reiterates that the donation and subsidized supply arrangements exclusion as proposed and as finalized in the offer health IT definition does not encompass any arrangement where an individual or entity does any of the following to or with any health IT that includes one or more certified Health IT Module(s):

- holds out the health IT for sale, resale, license, or relicense for deployment by or for other individual(s) or entity(ies);
- sells, resells, licenses, relicenses the health IT for deployment by or for other individual(s) or entity(ies); or
- otherwise provides or supplies the health IT for deployment by or for other individual(s) or entity(ies).

In other words, ONC draws a distinction between funding arrangements that will not meet the definition of "offer health IT", and arrangements where an individual or entity re-licenses or otherwise makes available the health IT itself to another healthcare provider, which would meet the definition. This distinction means that many EHR donation arrangements between hospitals and other healthcare providers (e.g., physicians) could continue to result in the hospital that donates health IT being deemed a health IT developer of certified health IT for purposes of the information blocking regulations. Additionally, ONC reminds stakeholders that donation and subsidized supply arrangements can implicate other laws, including the Federal Anti-Kickback Statute and nothing in this final rule should be construed as creating an exception to any fraud and abuse laws.

The finalized policy regarding the "donation and subsidized supply arrangements exclusion" from the offer health IT definition, ***explicitly and intentionally limits application of the donation and subsidized supply arrangements exclusion*** to those arrangements whereby the source of the subsidy makes available funding to cover costs of acquisition, augmentation, or upkeep of health IT. Additionally, it ***does not*** apply to sale, licensing, resale, relicensing, or provision or supply

[79] 88 FR 23859

of the health IT itself – regardless of whether such provision or supply is on subsidized or other terms. ONC reiterates that no individual or entity that otherwise meets the definition of any type of actor[80] "can opt out of being subject to information blocking regulations by engaging in any activity excluded from the offer health IT definition."

Finally, ONC states that it is "important for providers and other individual(s) or entity(ies) interested in engaging in any conduct that meets the offer health IT definition to note that engaging in such conduct makes the individual or entity one that offers health IT. **This means such an individual or entity will meet the health IT developer of certified health IT definition regardless of whether the individual or entity also happens to engage in any other conduct that is encompassed by an exclusion from the definition or that otherwise does not meet the offer health IT definition."**

Information Blocking Exceptions

Exceptions are voluntary and provide assurance to actors that, when a practice meets the exception, it will not constitute information blocking. ONC reminds actors seeking to satisfy an exception should review the exception's full regulatory text.[81] In addition, the requirements and conditions of each exception set forth in existing statute[82] should be read in context with the subpart's "availability and effect of exceptions" section[83], as well as the general provisions.[84] Where the conditions include any requirements the actor's practice must satisfy for an exception to apply, these requirements are included in that exception's section.[82]

In this final rule, ONC revised one condition and created two new conditions for the Infeasibility Exception. All of the conditions and requirements for the Infeasibility Exception to apply to an actor's practice of not fulfilling requested EHI access, exchange, or use due to the infeasibility of the request are specified in the final rule.[85]

ONC notes that the exceptions "are voluntary and offer an actor certainty that a practice that satisfies all of the relevant conditions of an exception will not be considered information blocking." They further reiterate "that failure to meet an exception does not necessarily mean a practice meets the definition of information blocking." By satisfying an exception, an actor gains the assurance that the actor's practice does not constitute information blocking. An actor's practice that does not meet the conditions of an exception does not automatically constitute information blocking, as the practice must still meet all the elements of the information blocking definition to be considered information blocking, including that the practice is likely to interfere with the access, exchange, or use of EHI, and that the actor acted with the requisite intent.[86]

ONC states that, where an actor engaging in a practice that is not (or practices that are not) fully covered by a single exception seeks certainty that such practices do not constitute information blocking, the actor could choose to satisfy several applicable exceptions that, in complement, do fully cover their practices. Applicable exceptions, and combinations of exceptions, will vary based on the actor's specific

[80] § 171.102
[81] Found in the exception's section of 45 CFR part 171
[82] Subparts B, C, and D of 45 CFR part 171
[83] 45 CFR 171.200, 45 CFR 171.300, and 45 CFR 171.400, respectively
[84] Subpart A of 45 CFR part 171
[85] § 171.204
[86] 85 FR 25820

practice and particular facts and circumstances in which they engage and the practices for which the actor seeks the certainty offered by information blocking exceptions.

ONC emphasizes that there may be a wide variety of scenarios where "stacking" combinations of various information blocking exceptions with one another, or with restrictions on use or disclosure of EHI under applicable law, may occur. **ONC will "issue additional guidance as needed and intend to propose additional exceptions in future rulemaking to further support health information privacy, including for information that patients may view as particularly sensitive such as reproductive health-related information."**

Infeasibility Exception – Uncontrollable Events & Third Party Seeking Modification Use Conditions

ONC has finalized a revision to the "uncontrollable events" condition which further clarifies when an actor's practice meets the "uncontrollable events" condition. The revision conveys that to meet this specific condition of the Infeasibility Exception with respect to any request, an actor cannot simply assert that they cannot fulfill a request because an "uncontrollable event"[87] occurred. To meet the condition, the actor must demonstrate that the uncontrollable event, in fact, negatively impacted the actor's inability to fulfill a request. Where this condition is met and the overall exception is met, it will not be considered information blocking when an actor does not fulfill a request to access, exchange, or use EHI that the actor cannot fulfill because of an uncontrollable event.

ONC has finalized, as proposed, the addition of a new "third party seeking modification use" condition. This condition permits actors to deny requests to modify EHI provided the request is not from a healthcare provider for which it is the business associate (BA). Where this condition is met and the overall exception is met, an actor's practice of not fulfilling a request for use of EHI will not be considered information blocking when:

- the actor is asked to enable a third party to modify EHI within the records or systems maintained by the actor; and
- the request is not from a healthcare provider (including a business associate acting on the healthcare provider's behalf) requesting such use from an actor that is its BA.

This new condition specifically focuses on requests to modify EHI held by or for a healthcare provider and is not applicable to third-party requests for other activities that would fall within the statutory definition[88] of the broader term "use." This condition was not proposed to apply, and as finalized does not apply, to an actor's practice of refusing to receive or process EHI via health information exchange or refusing to make EHI available for access, exchange, or use for permissible purposes. ONC clarifies that the third-party seeking modification use condition applies only where a third party seeks modification use functionality for EHI within the records or systems maintained by the actor. The third party seeking modification use condition is also not applicable to any request for "access" or "exchange" of EHI.[89]

The condition focuses on requests for a third party to have functionality to make modification use of EHI while, and as, it is held in the records or systems of the actor. ONC did not propose the condition to apply, and it cannot be met, where a third party is seeking to exchange EHI with the actor or to access

[87] Consistent with § 171.204(a)
[88] § 171.102
[89] As these terms are defined in § 171.102)

a copy of EHI, even if the actor may know or reasonably suspect that the third party may modify (or have modified) EHI that is in records, applications, or systems maintained by the third party.

The final rule notes that for purposes of this condition, an actor may choose to verify that the modification use request came from the healthcare provider themselves or accept the third party's representation of a request as coming from a healthcare provider. Any actor "considering whether to potentially avail themselves of the certainty offered by this exception will have flexibility to structure their communications approaches and operating procedures for communicating with the healthcare provider of which the actor is a BA, or with third parties representing themselves as BAs of such healthcare provider." According to ONC, this flexibility enables actors to operate and communicate efficiently while complying with the actor's obligations under the HIPAA Privacy Rule, other applicable law, and its binding agreements (including its BAAs) with the healthcare providers who choose to request third party modification use functionality either directly from the actor or through one of the healthcare provider's BAs.

In situations where an actor receives EHI via exchange from a third party, whether that EHI is reconciled and incorporated into the record ("added" to the record) is a determination for the healthcare provider and potentially its BAs. Any such exchange of EHI and subsequent determinations to reconcile and incorporate EHI into the record (or not) is not within the scope of the proposed condition. Additionally, "such practices and scenarios may implicate the information blocking definition, but there may also be other conditions or exception that apply depending on the specific facts and circumstances."

In addition to the examples ONC provided in the HTI-1 Proposed Rule and provided in this final rule describing the applicability of this condition, "they will continue to provide resources such as infographics, fact sheets, webinars, and other forms of educational materials and outreach." Resources specific to the information blocking regulations, across this and other ONC rules, are available on HealthIT.gov's Information Blocking website here.

Infeasibility Exception – Manner Exception Exhausted

ONC has finalized a new "manner exception exhausted" condition applies where an actor does not fulfill a request for access, exchange, or use of EHI after offering alternative, interoperable manners. This condition only applies under certain circumstances where the actor does not currently provide the requested manner of access, exchange, or use of the requested EHI to a substantial number of individuals or entities that are similarly situated to the requestor.

As discussed in the HTI-1 Proposed Rule, actors expressed uncertainty to ONC as to whether they have satisfied the infeasible under the circumstances condition in instances where they contended that fulfilling a request for access, exchange, or use of EHI would be infeasible.[90] Under the Infeasibility Exception, the infeasible under the circumstances condition requires the actor to demonstrate that complying with the request is infeasible when considering, among other things, the financial and technical resources available to the actor and why the actor was unable to provide access, exchange, or use of EHI consistent with the Manner Exception.

[90] 85 FR 23867

Specifically, actors have expressed concern about circumstances where the actor's inability to satisfy the Manner Exception's conditions rests solely on the requestor refusing to accept access, exchange, or use in any manner consistent with the statute[91], and fulfilling the request in the manner requested would require substantial technical or financial resources – or both – in the view of the actor, including significant opportunity costs.

ONC notes that they have observed this being more of a concern for actors with significant skills and other resources for developing unique technical solutions or new technological capabilities (e.g., EHR developers or HIN/HIEs) than for actors with few to no such resources (e.g., small clinician office practices or safety net clinics), because the infeasible under the circumstances condition of the Infeasibility Exception[92] requires actors to demonstrate their consideration of the financial and technical resources available to them, as well as why the actor was unable to provide access, exchange, or use of EHI.

Among those actors with substantial skills and other resources to develop new, unique or unusual manners of supporting access, exchange, or use of EHI – ONC has observed actors who appear to be experiencing a problematic level of uncertainty about whether they will be engaging in information blocking if they decline demands from requestors for non-standard or non-scalable solutions that they do not currently support even after they have offered to provide access exchange, or use of EHI in the same manner(s) the actor makes generally available to its customers or affiliates, and through standards-based manners[93] – including offering terms for such manners that are consistent with the Fees) and Licensing Exceptions.[94]

ONC stated in the HTI-1 Proposed Rule[95] that this new condition is necessary to ensure actors reasonably allocate resources toward interoperable, standards-based manners rather than allowing requestors, who, for whatever reason, do not build their products for compatibility with open consensus standards or other industry standards to attempt to force use of non-standard or non-scalable solutions by simply refusing to accept access, exchange, or use of EHI in any other manner.

ONC has proposed and finalized[96] a new condition in the Infeasibility Exception, the manner exception exhausted condition. Actors will be able to satisfy this exception when they have "exhausted" the manner requested condition and alternative manner condition of the Manner Exception and meet the other requirements of the new condition. If an actor either technically cannot provide the access, exchange, or use of EHI in the manner requested, or the actor and requestor cannot reach agreeable terms on the manner requested, then the actor must attempt to fulfill the request using the alternative manners.[97]

ONC has finalized the manner exception exhausted condition of the Infeasibility Exception with a requirement that an actor offer two alternative manners, at least one of which must be either of these alternative manners.[98] These alternative manners are, respectively, "[u]sing technology certified to

[91] § 171.301
[92] § 171.204(a)(5); previously § 171.204(a)(3)
[93] § 171.301
[94] § 171.302 and § 171.303
[95] 88 FR 23868
[96] § 171.204(a)(4)
[97] § 171.301(b) (85 FR 25877) (previously § 171.301(b)(2)(i)
[98] § 171.301(b)(1)(i) or (b)(1)(ii)

standard(s) adopted in part 170 that is specified by the requestor" (in other words, via health IT certified under the ONC Health IT Certification Program, 45 CFR part 170) or, "[u]sing content and transport standards specified by the requestor and published by: (A) the Federal Government; or (B) a standards development organization accredited by the American National Standards Institute."[99]

An actor may offer both of these alternative manners to satisfy this particular factor of the manner exception exhausted condition, or only one of these two and the manner specified,[100] which is "[u]sing an alternative machine-readable format, including the means to interpret the electronic health information, agreed upon with the requestor." If the actor offers the EHI in at least two manners including one of either of the alternative manners, then this factor of the finalized manner exception exhausted condition is satisfied.

ONC has finalized that the manner exception exhausted condition can be satisfied when an actor (who was unable to fulfill a request for access, exchange, or use of EHI because they could not reach an agreement with a requestor or were technically unable to fulfill the request in the manner requested) offered the requestor at least two alternative manners, one of which must use either technology certified to standard(s) adopted in part 170 that is specified by the requestor[101] or published content and transport standards consistent with statute.[102]

ONC has revised the condition to exclude certain factors from a "similarly situated" determination and has provided additional clarification and guidance. Specifically, they clarify that "similarly situated" cannot be used to discriminate against requestors based on whether the requestor is a competitor of the actor or whether the requestor will or might use the requested access, exchange, or use in a way that facilitates competition with the actor. An actor cannot discriminate in providing a form of access, exchange, or use of EHI that it currently provides to a substantial number of individuals or entities solely based on the requestor's status. ONC specifies[103] that such statuses include requests by individuals, and the healthcare provider type and size.

Previously, an actor who offered all the alternative manners would most likely look to the infeasible under the circumstances condition of the Infeasibility Exception – which requires actors to demonstrate that complying with the request is infeasible when considering many factors, including the cost to the actor of complying with the request in the manner requested and the financial and technical resources available to the actor. **The newly finalized manner exception exhausted "provides actors the option of satisfying the Infeasibility Exception without needing to assess whether they could meet the requestor's particularized demands regarding the manner and/or terms in which they want to obtain access, exchange, or use of the requested EHI."**

Additionally, because the October 6, 2022 date before which the "content" condition was relevant has now passed, the HTI-1 final rule revises the exception. The final rule removes the "content" condition as no longer necessary**; changes the name from "Content and Manner Exception" to "Manner Exception,";** and finalizes redesignation of paragraphs within the "Manner Exception" consistent with removal of the "content" condition.

[99] 45 CFR 171.301(b)(1)
[100] § 171.301(b)(1)(iii)
[101] § 171.301(b)(1)(i)
[102] § 171.301(b)(1)(ii)
[103] § 171.204(a)(4)(iv)

TEFCA Manner Exception

The HTI-1 final rule establishes a "TEFCA Manner" Exception that applies where an actor and requestor are both part of The Trusted Exchange Framework and Common Agreement (TEFCA). Where the exception is met, an actor's practice of fulfilling certain requests for access, exchange, or use of EHI only via TEFCA will not be considered information blocking.

Rather than include this condition as part of the Manner Exception, ONC has finalized a new subpart to the information blocking exceptions – Subpart D, "Exceptions That Involve Practices Related to Actors' Participation in The Trusted Exchange Framework and Common Agreement (TEFCA)."[104]

The new TEFCA Manner Exception provides that an actor's practice of limiting the manner in which it fulfills a request for access, exchange, or use EHI to provide such access, exchange or use only via TEFCA will not be considered information blocking when the practice follows these conditions (i.e., the finalized exception applies only where):

- the actor and requestor are both part of TEFCA;
- access, exchange, or use of the requested EHI can be supported via TEFCA for both the actor and requestor;
- the request for access, exchange or use is not via API standards adopted under the ONC Health IT Certification Program; and
- any fees charged and any licensing of interoperability elements by the actor in relation to fulfilling the request via TEFCA satisfy, respectively, the Fees Exception and Licensing Exception.

Rather than finalize the proposed definitions, in order to maintain consistency between the most current version of the Common Agreement and this regulation, ONC refers to the definitions used in the Common Agreement[105] for the terms used in this exception.

The first condition – that the actor and requestor are both part of TEFCA – simply means that both the actor and the requestor must be either a QHIN, Participant, or Subparticipant, as those terms are defined in the Common Agreement. This exception will not be available in any situation where the actor, or the requestor, is not a part of TEFCA.

The second condition requires that the requestor must be capable of receiving (accessing, exchanging, or using, depending on the requestor's request) the EHI from the actor, via TEFCA.

The third condition excludes requests from the exception where the requestor seeks to access, exchange, or use EHI via the "Application Programming Interface Standards,"[106] (or API standards) adopted by ONC on behalf of the Secretary or another version of those standards approved pursuant to the "Standards Version Advancement Process" (SVAP).[107] When a requestor seeks to access EHI via those API standards (essentially FHIR-based standards), an actor cannot use this exception. In other words, the third condition functions as a carve-out in that the exception is not available if the requestor requested access, exchange, or use of EHI via the API standards.

---

[104] § 171.403
[105] 88 FR 76773
[106] 45 CFR 170.215
[107] 45 CFR 170.405(b)(8)) under the ONC Health IT Certification Program

The fourth and final requirement for this condition states that any fees an actor charges, and any licensing terms an actor sets, must comply with the Fees Exception and the Licensing Exception.

Additional Resources & Quick Links

- ONC Resources on the Final Rule
  - ONC General Resources
  - Review the Final Rule
  - Press Release
- ONC Fact Sheets on the Final Rule
  - General Overview Fact Sheet
  - Final Rule At-a-Glance Fact Sheet
  - Decision Support Interventions and Predictive Models Fact Sheet
  - Insights Condition Fact Sheet
  - HTI-1 Information Blocking Fact Sheet
  - HTI-1 Key Dates Fact Sheet
- ONC Measurement Spec Sheets on the Final Rule
  - Individual Access Spec Sheet
  - C-CDA Reconcile Spec Sheet
  - Supported Apps Spec Sheet
  - Use of FHIR Spec Sheet
  - Use of FHIR Bulk Data Spec Sheet
  - Immunization Administrations Spec Sheet
  - Immunization Query Spec Sheet