SACHS POLICY GROUP

60 East 42nd Street, Suite 1762
New York, NY 10165
Phone: 212 827 0660
Fax: 212 827 0667

Interoperability, Information Blocking, and the ONC Health IT Certification Program Final Rule

OVERVIEW

On March 9th, the Department of Health and Human Services (HHS) Office of the National Coordinator for Health Information Technology (ONC) released a final rule titled "21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program." The rule updates health information technology (health IT) requirements and implements certain provisions of the 21st Century Cures Act. Among the most significant of these are requirements to make comprehensive electronic health information easily and quickly available upon request, along with descriptions of reasonable and necessary activities that do not constitute information blocking.

The final rule is available here.

CONDITIONS AND MAINTENANCE OF CERTIFICATION REQUIREMENTS

The rule establishes a number of Conditions and Maintenance of Certification requirements for health IT developers based on the requirements outlined in section 4002 of the Cures Act, which include the following:

- Information Blocking - A health IT developer cannot take any action that constitutes information blocking as defined in section 3022(a) of the Public Health Service Act (PHSA).
- Assurances - A health IT developer must provide assurances to the Secretary that, unless for legitimate purpose(s) as specified by the Secretary, will not take any action that constitutes information blocking as defined in section 3022(a) of the PHSA or any other action that may inhibit the appropriate exchange, access, and use of EHI.
- Communications - Developers are permitted to impose certain types of limited prohibitions and restrictions on certain communications, such as communications required by law, made to a government agency, or made to a defined category of safety organization. Developers certified under the Program may also place limitations on certain types of communications, including screenshots and video.
- Application Programming Interfaces (APIs) - The final rule adopts new standards, new implementation specifications, a new certification criterion, and modifies the Base EHR definition to implement the Cures Act API Condition of Certification requirement.
- Real World Testing - The rule establishes real world testing Condition and Maintenance of Certification requirements that include Maintenance of Certification requirements to update Health IT Modules certified to certain certification criteria to ensure certified technology meets its users' needs for widespread and continued interoperability. Real world testing Condition and Maintenance of Certification requirements apply to health IT developers with one or more Health IT Module(s) certified to specific certification criteria focused on interoperability and data exchange. Under these Condition and Maintenance of Certification requirements, health IT developers must submit publicly available annual real world testing plans as well as annual real world testing results for health IT.

- Attestations - The rule finalizes regulation text implementing the Cures Act's "attestations" Condition of Certification requirement, which requires that health IT developers attest twice a year to compliance with the Conditions and Maintenance of Certification requirements.
- Enforcement - The rule finalizes the proposed enforcement framework for the Conditions and Maintenance of Certification requirements, including the corrective action process for ONC to review potential or known instances where a Condition or Maintenance of Certification requirement under the Program has not been met or is not being met by a health IT developer.

Electronic Health Information (EHI) Export

The rule requires a certified Health IT Module to be able to electronically export a copy of all of the EHI that can be stored at the time of certification by the product. This provision was finalized with two primary use cases:

- To ensure that a patient's EHI is accessible to them and their designees, in a manner that facilitates communication with the patient's health care providers and other individuals, through the use of consumer-friendly software and third-party vendors; and
- To transfer complete historical data sets by a provider from one health IT system to another, such as upon changing electronic health record (EHR) vendors.

ONC defined the scope of data covered under the EHI export requirement to be the same protected health information that a patient would have the right to request under the HIPAA Privacy Rule. The failure to design a system able to export EHI, or the failure of a provider (actor) to export requested EHI constitutes information blocking unless one of the allowed exceptions is satisfied.

Application Programming Interfaces (APIs)

The final rule creates a new certification criterion which requires EHR developers to publish an API that facilitates the exchange of health data to and from their EHR system. API "read" capabilities, which allow authorized third parties to view data, must include both (1) services that provide access to a single patient's data and (2) services that provide access to multiple patients' data. APIs are not required to include "write" capabilities, which would allow authorized third parties to create or modify data.

The new API criterion requires the use of the HL7 Fast Healthcare Interoperability Resources (FHIR) standard Release 4 as well as several implementation specifications, which include:

- The HL7 FHIR US Core Implementation Guide STU 3.1.0 (US Core IG), instead of the originally proposed Argonaut Data Query Implementation Guide (Argonaut IG);
- The HL7 SMART Application Launch Framework Implementation Guide Release 1.0.0 (SMART IG), including mandatory support for the SMART on FHIR Core Capabilities;
- The HL7 FHIR Bulk Data Access Implementation Guide 1.0.0 (Bulk IG); and
- The OpenID Connect Core 1.0 standard.

It does not include the original proposal to adopt the API Resource Collection in Health (ARCH) specification due to concerns about being over-restrictive.

Specifically, to be certified by ONC, APIs must include the following functions:

- Enabling third-party apps to register with an authorization server;

- Establishing a secure connection with third-party apps, in accordance with the SMART IG and US Core IG specifications; and
- Authenticating and authorizing third-party apps to access data (including a new requirement for patients to be able to revoke access at any time).

EHR developers must also publicly supply complete documentation for their API. The rule also places conditions on the fees that developers can charge for use of their API technology. These conditions are largely unchanged from the original rule.

This criterion replaces the previous “Application Access—Data Category Request” certification criterion. However, ONC’s original proposal to also add a “Consent Management for APIs” criterion has not been adopted in the final version. Developers have 24 months to update their technology to make an API accessible. In the future, ONC expects that FHIR-enabled APIs may replace or complement CMS’s Quality Reporting Document Architecture (QRDA) standard.

INFORMATION BLOCKING EXCEPTIONS

Information blocking is defined as a practice that is likely to interfere with access, exchange, or use of EHI. If information blocking is conducted by a health information technology developer, health information network or health information exchange, such developer, network or exchange knows, or should know, that such practice is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information. If information blocking is conducted by a health care provider, that provider would have to know that such practice is unreasonable and is likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI.

The rule identifies eight activities as exceptions to the information blocking definition. The exceptions apply to certain activities that HHS deems likely to interfere with, prevent, or materially discourage the access, exchange, or use of EHI, but that would be reasonable and necessary if certain conditions are met.

The following five exceptions may be used to justify (temporarily or permanently) not fulfilling a request to access, exchange or use EHI:

1. **Preventing Harm**: if an actor has a reasonable belief that a practice will directly and substantially reduce the likelihood of a recognized harm to a patient or other person, the practice may not be information blocking. This exception is not triggered simply because the requested data would be accessed and analyzed actors without a patient-clinician relationship.
    1. Example: Processes intended to prevent inaccurate or corrupt patient data being recorded in an EHR
2. **Privacy**: if an actor is engaging in a reasonable and necessary practice intended to protect privacy. These practices must meet one of four identified sub-exceptions, which are designed to mirror existing practices under HIPAA.
    1. Example: Processes that respect requests from individuals not to share some or all of their patient information
3. **Security**: if an actor’s practices are directly related to safeguarding the confidentiality, integrity, and availability of EHI. These should implement an organizational security policy or a particular security determination.

   1. Example: Processes that are part of an industry security standard, such as the NIST Cybersecurity Framework

4. **Infeasibility**: if an actor is unable to comply with a request, or if the request would be unreasonably costly or burdensome. Actors must still make a timely response and a good faith effort to identify a reasonable alternative to the request.
   1. **Example**: Requests for data that cannot be unambiguously segmented from data that cannot be shared due to another exception, such as privacy or preventing harm, as in the case of a request that cannot unambiguously exclude patient records related to certain programs of treatment for substance abuse disorder.
5. **Health IT Performance**: if an actor temporarily makes EHI unavailable in order to maintain or improve the HIT system.

The following three exceptions may be to justify conditions placed on fulfilling a request to access, exchange or use EHI:

6. **Content and Manner**: if an actor limits the content of its response to all retained EHI specified in the USCDI, or if the actor is technically unable to fulfill the request in the manner requested or cannot come to agreeable terms. However, actors seeking to satisfy the 'manner' exception must provide alternative means to share EHI without undue delay that satisfies requestor content and transfer standards to the extent feasible (ONC provides a hierarchy of alternatives) and the reason for not coming to agreeable terms cannot be due to fees or licensing restrictions.

7. **Fees**: if an actor charges reasonable cost-related fees on an objective nondiscriminatory basis. Certain costs are specifically excluded from being reasonable, including any fee for an individual's electronic access to their own EHI.
8. **Licensing**: if an actor charges a reasonable and non-discriminatory fee for a license to use a health IT component (hardware or software).

An actor will not be subject to enforcement actions under the information blocking provision for civil monetary penalties or appropriate disincentives if they satisfy at least one exception. In order to satisfy an exception, an actor's practice must meet all conditions of an exception. Failing this, a practice would not have guaranteed protection from CMPs or appropriate disincentives, and would be evaluated on a case-by-case basis to determine whether information blocking has occurred.

OTHER UPDATES TO HEALTH IT CERTIFICATION CRITERIA

The final rule removes the 2014 Edition from the Code of Federal Regulations (CFR) due to its significantly outmoded standards and functionality, leaving the 2015 Edition as the sole standard for certification. The rule also reduces or removes several regulatory burdens from the current Program, including:

1. Removing the requirement to conduct randomized surveillance in the field on a set percentage of certified products, allowing ONC-Authorized Certification Bodies (ONC-ACBs). ONC-ACBs will still have the option to conduct randomized surveillance as they determine necessary or appropriate to support continued conformance to Program requirements by Health IT Modules they have certified.

2. Removing the ONC-Approved Accreditor (ONC-AA) from the ONC Health IT Certification Program in order to reduce the Program's administrative complexity and burden.
3. Removing certain Program requirements, including limitation disclosures and the Principle of Proper Conduct.
4. Removing certain other 2015 Edition certification criteria and standards, including the need to design and meet specific certification functionalities; prepare, test, and certify health IT in certain instances; adhere to associated reporting requirements; and maintain and update certifications for certified functionalities.

The final rule also updates the 2015 Edition to:

- Add two new technical certification criteria and two new attestation-structured privacy and security certification criteria; and
- Update some certification criteria to reflect changes to standards and implementation specifications.

Adoption of the United States Core Data for Interoperability (USCDI)

The rule finalizes the adoption of the USCDI standard for certification, which will establish a set of data classes and constituent data elements to support worldwide interoperability, and allow health IT developers to take advantage of a new proposed flexibility called the "Standards Version Advancement Process" (SVAP). SVAP will allow a developer to voluntarily have their products certified to newer National Coordinator approved versions of the USCDI in the future without waiting for rulemaking to update the version of the USCDI listed in the regulations.

USCDI will replace the Common Clinical Data Set (CCDS) 24 months after the publication date of this final rule. Specifically, the USCDI adds 3 new data classes, "Allergies and Intolerances," "Clinical Notes," and "Provenance," and adds the Patient Demographics data elements "Previous Address," "Phone Number," "Phone Number Type," and "Email Address" that were not defined in the CCDS. Finally, the USCDI adds pediatric vital signs data elements in order to satisfy requirements of the 21st Century Cures Act to improve use of health IT for the care of children.

Electronic Prescribing

The rule finalizes an update to the electronic prescribing National Council for Prescription Drug Programs (NCPDP) SCRIPT standard in from standard version 10.6 to standard version 2017071 for the electronic prescribing certification criterion. Additionally, the rule adopts the same electronic Prior Authorization (ePA) request and response transactions supported by NCPDP SCRIPT standard 2017071 proposed by CMS in the Medicare Program; Secure Electronic Prior Authorization for Medicare Part D proposed rule.

Clinical Quality Measures – Report Criterion

The rule removes the Health Level 7 (HL7) Quality Reporting Document Architecture (QRDA) standard requirements in the 2015 Edition "Clinical Quality Measures – Report" criterion and replaces them with required Health IT Modules to support the CMS QRDA Implementation Guide.

Privacy and Security Transparency Attestations

The rule adopts two new privacy and security certification criteria requiring transparency attestations from developers of certified health IT as part of the updated 2015 Edition privacy and security certification framework, which aims to identify whether or not certified health IT supports encrypting authentication credentials and/or multifactor authentication (MFA). New development will not be required at this time for health IT that does not meet these standards.

Security Tags and Consent Management

The rule changes the names of the two current 2015 Edition DS4P criteria to Security Tags - Summary of Care (Send) and Security tags - Summary of Care (Receive) and updates the requirements for these criteria to support security tagging at the document, section, and entry levels.

OTHER MODIFICATIONS TO THE HEALTH IT CERTIFICATION PROGRAM

The rule finalizes some simplifications to the ONC Health IT Certification Program:

- Removes the “Amendments” criterion for cases in which an IT function handles no patient data for which an amendment would be relevant;
- Makes corrections to certain aspects of the 2015 Edition privacy and security certification framework (80 FR 62705) and relevant regulatory provisions, in addition to the relevant current Certification Companion Guides (CCGs);
- Adopts new and revised Principles of Proper Conduct (PoPC) for ONC-ACBs and ONC-Authorized Testing Laboratories (ONC-ATLs); and
- Requires ONC-ACBs to accept test results from any ONC-Authorized Testing Laboratory (ONC-ATL) in good standing under the Program and compliant with the ISO/IEC 17025 accreditation requirements.