21st Century Cures Act: Interoperability, Information Blocking and ONC Health IT Certification

David S. Szabo
Co-Chair, Healthcare Practice Group

Massachusetts Health Data Consortium, CIO Forum

Agenda

- Burden Reduction and Deregulatory Actions
- Updates to Certification Criteria for CHIT
- Modifications to Certification Program
- Health IT Changes for Continuum of Care
- Maintenance of Certification
- Compliance & Enforcement
- Information Blocking (again)

Purposes Identified by ONC

- The purpose of the rule is to implement of key provisions in Title IV of the 21st Century Cures Act (Cures Act) that are designed to advance interoperability; support the access, exchange, and use of electronic health information (EHI); and address occurrences of information blocking.

Purposes

- The rule is intended to support patients' access to their EHI in a form convenient for patients, such as making a patient's EHI more electronically accessible through the adoption of standards and certification criteria and the implementation of information blocking policies that support patient electronic access to their health information at no cost.

Burden Reduction

- ONC: In this final rule, we have finalized new deregulatory actions that will reduce burden for health IT developers, providers, and other stakeholders:
  - (1) removal of a requirement to conduct randomized surveillance on a set percentage of certified products allowing ONC-Authorized Certification Bodies (ONC-ACBs) more flexibility to identify the right approach for surveillance actions;

Burden Reduction

- (2) removal of the 2014 Edition from the Code of Federal Regulations (CFR);
- (3) removal of the ONC-Approved Accreditor (ONC-AA) from the Program;
- (4) removal of certain 2015 Edition certification criteria; and
- (5) removal of certain Program requirements.

Updates to Certification

- Adoption of USCDI to replace CCD;
- Voluntary certification to new versions as new versions are introduced;
- E-prescribing updated to align with CMS Part D standards;
- Quality reporting updated to CMS, requirements, again to align with CMS reporting;.
- Required Electronic Health Information export for single patient EHI and for system replacements.

Updates to Certification

- API for single patient export and multiple patient export (HL7 FHIR Release 4);
- Privacy and security attestations by developers required; and
- Security tags and consent management: DS4P standard at the document, section, and entry levels of the record. Intended to help providers deal with sensitive information.

Continuum of Care

- Voluntary certification of health IT for pediatric care
- See www.healthit.gov/pediatrics
- RFI on modification of requirements to support cases for Opioid Use Disorder – comments from proposed rule under review

Maintenance of Certification

- Health IT developers or entities must adhere to certain Conditions and Maintenance of Certification requirements concerning:
- information blocking;
- appropriate exchange, access, and use of electronic health information;
- communications regarding health IT;

Maintenance of Certification

- application programming interfaces (APIs);
- real world testing;
- attestations regarding certain Conditions and Maintenance of Certification requirements;
- and submission of reporting criteria under the EHR reporting program under the Public Health Service Act.

Compliance

- ONC has created a framework for enforcing compliance with certification standards and other requirements imposed upon Health IT developers. The framework addresses:
  - A review process carried out by ONC;
  - Access to records;
  - Requirements for corrective actions;
  - Certification bans;
  - Appeals;
  - Suspensions;
  - Public listing of certification bans and suspensions; and
  - Coordination with Office of the Inspector General

Information Blocking

- A practice that is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information.
- If that practice is conducted by a health information technology developer, exchange, or network, such developer, exchange, or network knows, or should know, that such practice is likely to interfere with, prevent, or materially discourage the access, exchange, or use of electronic health information.
- If that practice is conducted by a health care provider, such provider knows that such practice is unreasonable and is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information.

Information Blocking

- The information blocking practices may include:
- Practices that restrict **authorized** access, exchange, or use under applicable State or Federal law of such information for treatment and other permitted purposes under such applicable law, including transitions between certified health information technologies;
- Implementing health information technology in nonstandard ways that are likely to substantially increase the complexity or burden of accessing, exchanging, or using electronic health information; and

Information Blocking

- Implementing health information technology in ways that are likely to restrict the access, exchange, or use of electronic health information **with respect to exporting complete information sets or in transitioning between health information technology systems**; or

- Or in ways that lead to fraud, waste, or abuse, impede innovations and advancements in health information access, exchange, and use, including care delivery enabled by health information technology.

- There are eight exceptions.

Preventing Harm

- This exception is intended to prevent harm to a patient or another person, by protecting them against the substantial risk of harm otherwise arising from the access, exchange or use of EHI. The risk itself must be “substantial.”

- ONC intends that this standard be aligned with HIPAA rules regarding giving patients access to their medical records when it is applied to covered entities and business associates.

Preventing Harm

- The ONC rule also addresses circumstances under which a risk to **life or physical safety** would arise if EHI is misidentified or mismatched, corrupt due to technical failure or erroneous.

- Organizations are permitted to create an organizational policy to meet the prevention of harm standard, but the policy must be developed with input from clinical, technical and other relevant staff, be implemented on a consistent basis and be no broader than necessary to mitigate the risk of harm.

Privacy Exception

- Actions to block the flow of EHI in order to protect an individual's privacy rights must be consistent with HIPAA, the Part 2 rules, applicable state law and other privacy law and policies. It has four sub-exceptions:
  - When a consent or other permission required by law has not been provided (typically applies to CEs and BAs);
  - For healthcare IT developers not covered by HIPAA but who have consumer-facing privacy policies;
  - When denial of access if permitted by HIPAA; and
  - When denial of access if based on the request of the subject of the information.

Security

- ONC contemplates that each holder of EHI will implement its own security safeguards appropriate to its size and structure (i.e. scalable).
- The purpose of the Security Exception is to permit reasonable and necessary information security practices that do not unreasonably interfere with access, use or exchange of EHI.
- Adherence to security policies that reflect consensus-based standards is unlikely to be deemed information blocking.

Infeasibility Exception

- This exception is meant to capture “legitimate practical challenges” beyond an entity’s control that limit its ability to comply with requests to access, exchange or use EHI.
- Practical challenges can include: technological capability, legal rights, financial resources’ or other means necessary to comply.
- An infeasible request imposes a substantial burden, that is unreasonable for the entity to assume.

Infeasibility Exception

- To meet this exception, the holder of the information must be subject to either:
  - an uncontrollable event, such as a disaster, public health emergency, public safety incident, war, terrorist attack, insurrection, labor unrest, telecommunication interruption or act of a regulatory authority; *or*
  - A portion the requested information should be withheld because of applicable law, lack of consent or risk of harm, and the holder can segment the information that can be disclosed from the information that should not be disclosed.
  - Or . ..

Infeasibility

- Fulfillment of the request is otherwise infeasible taking into account a six-factor test set forth in the regulations.

- If the request is infeasible to fulfill, the holder must notify the requestor in ten business days of the reasons why the request in infeasible.
- This is intended to be a narrow exception, not easily applied.

Health IT Performance Exception

This exception has four conditions, and meeting any one of them triggers the exception:

- Unavailability of EHI as a result of planned or unplanned maintenance or updates of IT systems, applied in a non-discriminatory manner by the a health IT developer, HIE, or HIN.
- Unavailability of EHI to a particular third-party app that is negatively-impacting system performance;
- Unavailability to in response to a risk of harm; or
- Unavailable of EHI based on an information security risk.

Content and Manner of Exchange

- For the first 24 months after the effective date of the rule, a holder of data may limit the **content** of the response to the USDCI standard data set. https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi

- Subsequently, all EHI in the possession of the holder must be produced.

Content and Manner of Exchange

- A holder should fulfill the request in the manner requested, unless the holder is technically unable to do or cannot reach agreement on terms to so with the requestor.

- If the holder satisfies the request in the manner requested, then the rules regarding fees and licensing terms do not apply.

Content and Manner of Exchange

- If the request is not fulfilled in the manner requested due to technical issues or a failure to reach agreement, then the holder shall fulfill the request as follows:
  - If possible, using certified technology specified by the requestor;
  - Or if not, using transport standards specified by the Federal Government or using an ANSI standard;
  - Or if not, using an alternative machine-readable format.
- PROVIDED that the limitations on fees and licensing terms shall then apply.

Fees

- Fees for fulfilling a request of EHI are permitted as follows:
  - Uniformly applied and based on objective and verifiable criteria;
  - Reasonably related to costs and a reasonable profit margin;
  - Reasonably allocated among similarly situated persons or entities;
  - Based on costs not already recovered for the same instance of service to a provider or a third party.

Fees

- Fees cannot be based upon:
  - Whether the requestor is a competitor, potential competitor, or someone who might facilitate competition;
  - The sales, profit or value the requestor might realize from the data requested;
  - Costs incurred due to fulfilling the request in a non-standard way, unless requestor agreed to the fee;
  - Costs associated with intangible assets;
  - Opportunity costs; or
  - Costs that led to creation of intellectual property

Fees

- The “Fees” exception to the information blocking rule does not apply to:
  - Fee limitations or prohibitions in the HIPAA privacy rule
  - A fee charged to export ePHI from certified health IT for the purposes of changing IT systems or providing ePHI to a patient; or
  - A fee to convert data from an electronic health record that was not agreed to when the record system was acquired.

Licensing Exception

- Charging a licensing fee for technology needed for interoperability is permitted if:
  - Negotiations are commenced within ten days of a request and are completed within thirty days;
  - The scope of rights granted must be sufficient to enable the exchange of EHI as intended;
  - The royalty must be reasonable, non-discriminatory and based on the value of the technology licensed; and
  - The royalty cannot be charged if the developments costs have already been recovered as part of a permitted fee.

Questions?

David S. Szabo

Locke Lord LLP

David.Szabo@lockelord.com

617-239-0414