GENERAL COMMITTEE MEETING

Thursday, February 21, 2019

3:00 PM to 4:00 PM

Healthcare Leadership Council

750 9th Street, NW, Suite 500 Washington, D.C. 20001

Conference Line: 857-232-0157, **Code:** 30-40-73

1. **Welcome and Introductions**

2. **Proposed Rules** **Attachment**
   ONC: Information Blocking Interoperability, Information Blocking, and the ONC Health IT Certification Program

   CMS: Interoperability & Patient Access

3. ***Privacy Hearings***
   Senate Commerce Hearing on Policy Principles for a Federal Data Privacy Framework in the United States —2/27

   House Energy & Commerce Hearing on Protecting Consumer Privacy in the Era of Big Data—2/26

The Office of the National Coordinator for Health Information Technology

21ST CENTURY CURES ACT:
INTEROPERABILITY, INFORMATION BLOCKING, AND
THE ONC HEALTH IT CERTIFICATION PROGRAM PROPOSED RULE

Seven Exceptions to the Information Blocking Provision

OVERVIEW

- Section 4004 of the Cures Act authorizes the Secretary of Health and Human Services to identify reasonable and necessary activities that do not constitute information blocking.
- In consultation with stakeholders, we have identified seven categories of practices that would be reasonable and necessary, provided certain conditions are met.
- The seven categories of reasonable and necessary practices, and their corresponding conditions, are defined through the exceptions proposed at 45 CFR 171.201–207.
- If the actions of a regulated actor (health care provider, health IT developer, or health information exchange or network) satisfy one or more exception, the actions would not be treated as information blocking and the actor would not be subject to civil penalties and other disincentives under the law.

"Actors" regulated by the information blocking provision:

- Health Care Providers
- Health IT Developers of Certified Health IT
- Health Information Exchanges
- Health Information Networks

§ 171.201 Exception | Preventing Harm

- An actor may engage in practices that are reasonable and necessary to prevent physical harm to a patient or another person.
- The actor must have a reasonable belief that the practice will directly and substantially reduce the likelihood of physical harm to a patient or another person.
- The practice must implement an organizational policy that meets certain requirements or must be based on an individualized assessment of the risk in each case.

This proposed exception acknowledges that the public interest in protecting patients and other persons against unreasonable risks of harm can justify practices that are likely to interfere with access, exchange, or use of electronic health information (EHI).

§ 171.202 Exception | Promoting the Privacy of EHI

- An actor may engage in practices that protect the privacy of EHI.
- An actor must satisfy at least one of four discrete sub-exceptions that address scenarios that recognize existing privacy laws and privacy-protective practices: (1) practices that satisfy preconditions prescribed by privacy laws; (2) certain practices not regulated by HIPAA but which implement documented and transparent privacy policies; (3) practices that are specifically permitted under HIPAA; (4) practices that give effect to an individual's privacy preferences.
- The information blocking provision will not require that actors provide access, exchange, or use of EHI in a manner that is not permitted under the HIPAA Privacy Rule.
- General conditions apply to ensure that practices are tailored to the specific privacy risk or interest being addressed and implemented in a consistent and non-discriminatory manner.

This proposed exception would advance the goal of preventing information blocking for improper or self-interested purposes while maintaining and upholding the privacy rights that patients now have.

§ 171.203 Exception | Promoting the Security of EHI

- An actor may implement measures to promote the security of EHI.
- The practice must be directly related to safeguarding the confidentiality, integrity, and availability of EHI.
- The practice must be tailored to specific security risks and must be implemented in a consistent and non-discriminatory manner.
- The practice must implement an organizational security policy that meets certain requirements or must be based on an individualized determination regarding the risk and response in each case.

This proposed exception would protect actors who mitigate security risks and implement appropriate safeguards to secure the EHI they control.

§ 171.204 Exception | Recovering Costs Reasonably Incurred

- An actor may recover costs that it reasonably incurs, in providing access, exchange, or use of EHI.
- Fees must be: (1) charged on the basis of objective and verifiable criteria uniformly applied to all similarly situated persons and requests; (2) related to the costs of providing access, exchange, or use; and (3) reasonably allocated among all customers that use the product/service.
- Fees must not be based on anti-competitive or other impermissible criteria.
- Certain costs would be specifically excluded from coverage under this exception, such as costs that are speculative or subjective, or costs associated with electronic access by an individual to their EHI.

This proposed exception acknowledges that actors should be able to recover costs that they reasonably incur to develop technologies and provide services that enhance interoperability and promote innovation, competition, and consumer welfare.

§ 171.205 Exception | Responding to Requests that are Infeasible

- An actor may decline to provide access, exchange, or use of EHI in a manner that is infeasible.
- Complying with the request must impose a substantial burden on the actor that is unreasonable under the circumstances (taking into account the actor's size, resources, etc.).
- The actor must timely respond to infeasible requests and work with requestors to provide a reasonable alternative means of accessing the EHI.

This proposed exception acknowledges that there may be legitimate practical challenges beyond an actor's control that may limit its ability to comply with requests for access, exchange, or use of EHI.

§ 171.206 Exception | Licensing of Interoperability Elements on Reasonable and Non-discriminatory Terms

- An actor that controls technologies or other interoperability elements that are necessary to enable access to EHI will not be information blocking so long as it licenses such elements on reasonable and non-discriminatory terms.
- The license can impose a reasonable royalty but must include appropriate rights so that the licensee can develop, market, and/or enable the use of interoperable products and services.
- The terms of the license must be based on objective and verifiable criteria that are uniformly applied and must not be based on impermissible criteria, such as whether the requestor is a potential competitor.

This proposed exception would allow actors to protect the value of their innovations and earn returns on the investments they have made to develop, maintain, and update those innovations.

§ 171.207 Exception | Maintaining and Improving Health IT Performance

- An actor may make health IT under its control temporarily unavailable in order to perform maintenance or improvements to the health IT.
- An actor must ensure that the health IT is unavailable for no longer than necessary to achieve the maintenance or improvements.
- In circumstances when health IT is supplied to an individual or entity, the individual or entity (e.g., customer) must agree to the unavailability of health IT.

The proposed exception recognizes that it may be reasonable and necessary for actors to make health IT, and in turn EHI, temporarily unavailable for the benefit of the overall performance of health IT.

Fact sheet

CMS Advances Interoperability & Patient Access to Health Data through New Proposals

Feb 08, 2019

CMS Advances Interoperability & Patient Access to Health Data through New Proposals

Today, February 11, 2019, the Centers for Medicare & Medicaid Services (CMS) proposed policy changes supporting its MyHealthEData initiative to improve patient access and advance electronic data exchange and care coordination throughout the healthcare system. The Interoperability and Patient Access Proposed Rule outlines opportunities to make patient data more useful and transferable through open, secure, standardized, and machine-readable formats while reducing restrictive burdens on healthcare providers.

In addition to the policy proposals, CMS is releasing two Requests for Information (RFIs) to obtain feedback on interoperability and health information technology (health IT) adoption in Post-Acute Care (PAC) settings, and the role of patient matching in interoperability and improved patient care.

“For far too long, electronic health information has been stuck in silos and inaccessible for healthcare consumers,” said CMS Administrator Seema Verma. “Our proposals help break down existing barriers to important data exchange needed to empower patients by giving them access to their health data. Touching all aspects of healthcare, from patients to providers to payers and researchers, our work leverages identified technology and standards to spark new opportunities for industry and researchers while improving healthcare quality for all Americans. We ask that members of the healthcare system join forces to provide patients with safe, secure access to, and control over, their healthcare data.”

CMS will accept comments on the major provisions in this proposed rule and the RFIs (CMS-9115-P) until early April (exact date will be updated upon posting at the Federal Register); it can be downloaded from the **Federal Register** at: https://www.federalregister.gov/public-inspection.

Proposed Changes and Updates

Patient Access Through Application Programming Interfaces (APIs)
The MyHealthEData initiative empowers patients by ensuring access and use of their healthcare data while keeping it safe and secure. Having timely electronic access to health information makes it easier for people to make more informed decisions about their healthcare needs.

Last year, we launched the Blue Button 2.0 application programming interface (API) in Medicare fee-for-service (FFS), allowing beneficiaries to access their health claims information electronically through the application of their choosing. CMS currently has over 1500 application developers building tools with this API. Because health information is useful to patients, and we are interested in providing individuals with access to their health information, similar to CMS' approach to Blue Button 2.0, we are proposing to require Medicare Advantage (MA) organizations, state Medicaid and CHIP FFS programs, Medicaid managed care plans, CHIP managed care entities, and QHP issuers in FFEs to implement, test, and monitor an openly-published Health Level Seven (HL7®) Fast Healthcare Interoperability Resources (FHIR®)-based APIs to make patient claims and other health information available to patients through third-party applications and developers.

Health Information Exchange and Care Coordination Across Payers
As patients move throughout the healthcare system, in particular from payer to payer, they should be able to maintain access to their healthcare information. We are proposing to require MA organizations, Medicaid managed care plans, CHIP managed care entities, and QHP issuers in the FFEs to support electronic exchange of data for transitions of care as patients move between these plan types. This data includes information about diagnoses, procedures, tests and providers seen and provides insights into a beneficiary's health and healthcare utilization. By ensuring patients have access to their information, and that information follows them on their healthcare journey, we can reduce burden, eliminate redundant procedures and testing, and give back valuable clinician time to focus on improving care coordination, and ultimately health outcomes. A total of approximately 125 million Americans would have access this important health information if this proposal is finalized.

API Access to Published Provider Directory Data
Health plan provider directories help patients find in-network providers and allow healthcare professionals to locate other providers for access to medical records, referrals, transitions of care, and care coordination. To ensure patients and providers have easy access to this information, we are proposing to require MA organizations, state Medicaid and CHIP FFS programs, Medicaid managed care plans, and CHIP managed care entities to make their provider networks available to enrollees and prospective enrollees through API technology. APIs ensure that up to date information for all providers is available for use by developers building tools to support beneficiaries. Because QHP issuers on the Federally Funded Exchanges are already required to make provider directory information available in a specified, machine-readable format, we are not proposing these requirements for QHP issuers at this time.

Care Coordination Through Trusted Exchange Networks
Exchanging health information on the internet requires a reliable 'trust framework' that verifies the security and identity of participants. Trust networks are those in which plans and providers can share information freely no matter what health information IT network they belong to. However, there are a limited number of networks today, and there is a need to expand and integrate more plans and providers into these networks. We propose that payers in CMS programs be able to participate in a trusted exchange network which would allow them to join any health information network they choose and be able to participate in nationwide exchange of data. This would enable the information to flow securely and privately between plans and providers throughout the healthcare system. We propose requiring MA organizations (including MA-PD plans), Medicaid managed care plans, CHIP managed care entities, and QHP issuers in the FFEs to participate in trust networks to improve interoperability.

Improving the Dual Eligible Experience by Increasing Frequency of Federal-State Data Exchanges
CMS proposes an update on the frequency with which states are required to exchange certain Medicare/Medicaid data on dually eligible beneficiaries from a monthly exchange to a daily exchange to improve benefit coordination for the dual eligible population. The data exchanged include files of all eligible Medicaid beneficiaries by state, as well as "buy-in" data, or information about beneficiaries states are using Medicaid funds to "buy-in" Medicare services. Additionally, we seek public comment for consideration in future rulemaking on how we can achieve greater interoperability of federal-state data for dually eligible beneficiaries.

Public Reporting and Prevention of Information Blocking
Practices that unreasonably limit the availability, disclosure, and use of electronic health information undermine efforts to improve interoperability. We believe it would benefit patients and caregivers to know if individual clinicians, hospitals, and critical access hospitals (CAHs) have submitted a "no" response to any of the three attestation statements regarding the prevention of information blocking in the Promoting Interoperability Programs. Making this information publicly available may motivate clinicians, hospitals, and CAHs to refrain from information blocking.

Provider Digital Contact Information
Electronic addresses allow providers to exchange data faster while improving interoperability and could eliminate the need for fax machines for the exchange of health information. A centralized directory of provider electronic addresses for data exchange could ensure the flow of patient information and any needed provider-to-provider communication is seamless for all users. The 21st Century Cures Act required the Secretary to create a provider digital contact information index, and as of June 2018, the National Plan and Provider Enumeration System (NPPES) has been updated to include one or more pieces of digital contact information that can be used to facilitate secure sharing of health information. To ensure that the NPPES is updated with this information, CMS is proposing to publicly report the names and National Provider

Identifiers (NPIs) of those providers who have not added digital contact information to their entries in the NPPES system beginning in the second half of 2020.

Revisions to the Conditions of Participation (CoPs) for Hospitals and Critical Access Hospitals
The CoPs for hospitals and CAHs set basic health and safety standards for how effective care transitions for discharged patients should occur. Electronic patient notifications are a proven tool for improving transitions of care between settings and improving patient safety. While deploying these notifications is low-cost and easy to achieve with any electronic health record system, many hospitals have not developed capabilities to send these notifications to other providers and facilities to whom they transition patients. We propose requiring Medicare-participating hospitals, psychiatric hospitals, and CAHs to send electronic notifications when a patient is admitted, discharged or transferred.

Advancing Interoperability in Innovative Models
The Center for Medicare and Medicaid Innovation ("Innovation Center") models are an important lever to advance interoperability. The Innovation Center is seeking public comment on promoting interoperability among model participants and other healthcare providers as part of the design and testing of innovative payment and service delivery models.

These models offer a unique opportunity to engage with healthcare providers in innovative ways and test new concepts. CMS plans to promote interoperability across the healthcare spectrum through model testing that focuses on using emerging standards, models leveraging non-traditional data and technology-enabled patient engagement platforms.

Requests for Information

CMS is looking for ways to facilitate private sector work on a practical and scalable patient matching strategy. Together with the *Office* of the *National Coordinator* for *Health* Information Technology (ONC), CMS is requesting feedback on how it can leverage its authority to improve patient identification and safety to encourage better coordination of care across different healthcare settings while advancing interoperability.

In addition, we are requesting input on how CMS can promote wide adoption of interoperable health IT systems for use across healthcare settings such as long-term and post acute care, behavioral health, and settings serving individuals who are dually eligible for Medicare and Medicaid and/or receiving home and community-based services.

The RFIs continue the national conversation about improving the healthcare delivery system and includes how CMS can:

- Promote interoperability
- Reduce burden for clinicians, providers, and patients, while encouraging care coordination, and
- Lead change to a value-based healthcare system.

Stakeholder input is encouraged for consideration in future regulatory action to improve quality of care, decrease costs, make the healthcare system more effective, and bring positive solutions that achieve transparency, flexibility, program simplification, and innovation.

In responding to the RFIs, commenters should provide CMS with clear and concise proposals that include data and specific examples. Analysis regarding CMS' authority is welcome, particularly if proposals involve novel legal questions. CMS will not respond to RFI comment submissions in the final rule, but will actively consider all input in developing future regulatory proposals and/or sub-regulatory guidance.

To receive more information about CMS's interoperability efforts, sign-up for listserv notifications,
here: https://public.govdelivery.com/accounts/USCMS/subscriber/new?topic_id=USCMS_12443

To view the proposed rule (CMS-9115-P), please
visit: https://www.federalregister.gov/public-inspection