21st Century Information Sharing: Patient Access & Information Blocking

Consumer Webinar
March 28, 2019

national partnership for women & families

Overview

- **Long-awaited rules on patient access and information blocking from CMS and ONC**
  - CMS Interoperability & Patient Access Proposed Rule
  - ONC Interoperability & Information Blocking Proposed Rule
- **Overview: Proposals are wide-reaching and would have an impact on all facets of the health care system.**
  - Patients and caregivers
  - Clinicians and hospitals
  - Payers
- **Comments Due: Friday, May 03, 2019**

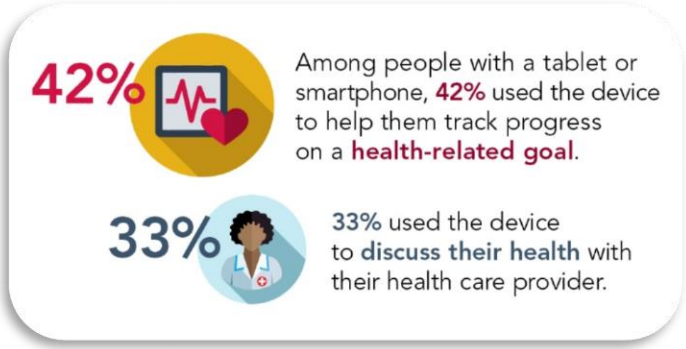
CMS: Background & history

- **CMS Interoperability & Patient Access Proposed Rule**
  - "Improve access to, and the quality of, information that Americans need to make informed health care decisions, including data about health care prices and outcomes, while minimizing reporting burdens."
- **Value-based care**
  - Health Care Choice and Competition EO
- **Empowered patients, better decisions:**

"Helping to inform patient choice of coverage options and care providers to **more effectively manage their own health, care, and costs**."

CMS: Patient access through APIs

- **APIs = New mechanisms for secure patient access via mobile devices**
  - Application Programming Interfaces (APIs) allow health apps to access health data
- **Previous efforts to share clinical data via APIs**
  - Clinicians and hospitals via "Meaningful Use" requirements
- **PROPOSAL: New focus on claims (and other) data**
  - Health plans unique position to provide a complete picture of health care history
  - Piecing together claims and encounter data from across the system



CMS: Patient access through APIs

Who is Sharing?

- **Require payers to implement APIs to share information with enrollees and beneficiaries:**
  - MA organizations
  - Medicaid Managed Care plans
  - CHIP managed care entities & agencies that operate FFS systems
  - Medicaid state agencies
  - Issuers of QHPs in the FFEs

What Data?

- **Claims and encounter data**
  - Adjudicated claims (including cost)
  - Encounters with capitated providers
  - Provider remittances
  - Enrollee cost-sharing
- **Provider directory data**
  - Provider names, addresses, phones numbers and specialty
- **Clinical data, including lab results (where available)**
  - Any clinical data in the USCDI standard
- **Drug benefit data**
  - Pharmacy directory data (#, mix, addresses)
  - Formulary/preferred drug list data

CMS: Privacy & security in the context of APIs

- **Reminder: Boundaries of HIPAA**
  - HIPAA does not apply to information downloaded/stored on people's mobile devices.
  - Covered entities are not responsible under the HIPAA rules for the security of PHI once it has been received by an application (app) chosen by an individual.
- **PROPOSAL: Make available to current and former enrollees information and resources about:**
  - Selecting a health app
  - Practical strategies to safeguard data
  - How to submit complaints to OCR and FTC
- **Enrollee and beneficiary resources regarding privacy and security:**
  - Must be made available on the organization's website
  - Information must be available in non-technical, consumer-friendly language
  - Organizations can choose to use existing HHS or FTC resources

CMS: Take your data with you when you go

- **PROPOSAL: Coordinate care between plans by exchanging, at a minimum, the data elements in the United States Core Data for Interoperability (USCDI) Standard**
- **Upon enrollee request:**
  - (1) Accept the data set from another plan that covered the enrollee within the previous five years
  - (2) Send the data at any time during an enrollee's enrollment and up to five years later to enrollee's current plan
  - (3) Send the data at any time during enrollment or up to five years after enrollment has ended to a recipient identified by the employee

USCDI v1:

- ✓ Assessment and plan of treatment
- ✓ Care team members
- ✓ Clinical notes
- ✓ Patient goals
- ✓ Health concerns
- ✓ Immunizations
- ✓ Laboratory
- ✓ Medications
- ✓ Patient demographics
- ✓ Problems
- ✓ Procedures
- ✓ Provenance
- ✓ Smoking status
- ✓ Unique Device Identifier (*for implantable devices*)
- ✓ Vital Signs

CMS: Patient event notifications

- **PROPOSAL: Revise Conditions of Participation for hospitals to require these entities to send patent event notifications of a patient's admission, discharge, and/or transfer to another health care facility or community provider.**
  - Personal or demographic information
  - Name of the sending institution
  - Diagnosis (if not prohibited by applicable law)
- **Limited to hospitals which currently posses EHR systems with the necessary technical capacity**
- **Seeking comment on whether to identify a broader set of patients outside of those admitted and seen as inpatients**
  - E.g., Emergency room visits

CMS: Other proposals

- **Require certain plans to participate in a trusted health information exchange network**
  - MA organizations,
  - Medicaid and CHIP managed care entities,
  - QHP issuers in FFEs
- **Test ways to promote interoperability across the health care spectrum through models tested by the Center for Medicare & Medicaid Innovation**
- **Improve the dually-eligible experience by increasing frequency of Federal-State data exchanges**
  - Require all states to participate in daily exchange of buy-in data to CMS
- **COMING SOON: Updates to the Promoting Interoperability Program (AKA "Meaningful Use") for eligible hospitals**

CMS: Information blocking

- **PROPOSAL: Publicly report the names of eligible clinicians and hospitals who do not answer "no" to information blocking attestation statements**
  - Names made available on Physician Compare; CMS websites available to the public
  - Incomplete attestations (e.g., statements left blank) would not be listed online
- **PROPOSAL: Publicly identify clinicians who have not submitted digital contact information in NPPES**
  - To increase the number of clinicians with valid and current digital contact information available through NPPES

Information Blocking Attestations:

1) Did not knowingly and willfully take action to limit or restrict the compatibility or interoperability of CEHRT.

2) Acted in good faith to implement CEHRT in a way that supported and did not restrict access to the exchange of electronic health information.

3) Acted in good faith to use CEHRT to support the appropriate exchange and use of electronic health information.

ONC: Background & history

- **Purpose:**
  - Increase choice and competition
  - Reduce burden and advance interoperability
  - Promote patient access
- **2014: Congress asks ONC to investigate information blocking**
- **2015: ONC submits report to Congress on health information blocking**
- **2016: 21st Century Cures Act signed into law**
  - Definition of information blocking
  - Define exceptions
  - OIG Enforcement
    - Penalties for some actors
    - "Disincentives" for providers
- **2019: Proposed rule released**

Information blocking

- **Information Blocking**
  - A practice that – except as required by law or specified by the Secretary as a reasonable and necessary activity – is likely to interfere with, prevent, or materially discourage access, exchange or use of electronic health information
- **Who: Actors**
  - Health care providers
  - Health IT developers of certified health IT
  - Health Information Exchanges (HIEs)
  - Health Information Networks (HINs)

Electronic Health Information

- **PROPOSAL: Electronic health information (EHI) to be defined as any information that:**
  - Is transmitted by or maintained in electronic media
  - Identifies the individual (or can be used to identify them)
  - Relates to the past, present, or future health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual.
- **Not limited to information created/received by a health care provider**
- **Does not include de-identified health information**
- **EHI > Protected Health Information (PHI)**

Price information – request for information

- **REQUEST for COMMENT: Parameters and implications of Including price information within the scope of EHI for purposes of information blocking**
- **What:**
  - Should prices reflect the amount to be charged to and paid for by the patient's health plan (if the patient is insured) and the amount to be charged to and collected from the patient (as permitted by the provider's agreement with the patient's health plan), including for drugs or medical devices?
  - Should pricing information reflect all out-of-pocket costs such as deductibles, copayments and coinsurance (for insured patients)?
- **How:**
  - Are there electronic mechanisms/processes available for providing price information to patients who are not registered (i.e., not in the provider system) when they try to get price information?
  - Should price information be made available on public websites so that patients can shop for care without having to contact individual providers, and if so, who should be responsible for posting such information?
  - How can price transparency be achieved for care delivered through value based arrangements, including at accountable care organizations, demonstrations and other risk-sharing arrangements?

Price information – continued

- **REQUEST for COMMENT: Parameters and implications of including price information within the scope of EHI for purposes of information blocking**
- **When:**
  - Should prices that are included in EHI be reasonably available in advance and at the point of sale?
  - To the extent that patients have a right to price information within a reasonable time in advance of care, how would such reasonableness be defined for:
    - Scheduled care (including for patients still shopping for care);
    - Emergency care
    - Ambulance services, including air ambulance services; and
    - Unscheduled inpatient care
- **Other:**
  - If price information is included in EHI, could that information be useful in subsequent rulemaking that the Department may consider in order to reduce or prevent surprise medical billing?

Information blocking categories

Categories of practice "likely to interfere" with access/exchange/use of EHI

1. **Restrictions on access, exchange, or use**
2. **Limiting or restricting the interoperability of health IT**
3. **Impeding innovations and advancements in access, exchange or use of health IT**
4. **Rent-seeking and other opportunistic pricing practices**
5. **Non-standard implementation practices**

Examples of information blocking

- **A health IT developer charges customers fees, throttles speeds, or limits the number of records users can export when exchanging EHI with competing EHR products**
- **A health care provider has the ability to provide same-day access to EHI but takes several days to respond**
- **A developer will only provide EHI in PDF format even though it can produce the data in a commercially reasonable structured format**
- **A health system's internal policies require staff to obtain the patient's written consent to share EHI with unaffiliated provider even though that is not required by state or federal law**

7 Exceptions

Reasonable and necessary practices that do not constitute information blocking:

1. **Preventing Harm**
2. **Promoting the Security of EHI**
3. **Promoting the Privacy of EHI**
4. **Cost Recovery**
5. **Responding to Infeasible Requests**
6. **Licensing Interoperability Requirements**
7. **Maintaining and Improving health IT Performance**

7 Exceptions, continued

- **Conditions:** All applicable conditions of the exception must be met at all relevant times and for each practice in order to qualify
- Organizational policy/procedure:
  - Must be in writing
  - Be developed with meaningful input from clinical, technical and other appropriate staff
  - Implemented in a consistent and non-discriminatory manner
  - No broader than necessary for the specific risk or type of risk at issue
- Subject to qualifying individualized finding
  - A justifiable case-by-case basis

7 Exceptions, continued

- **1. Preventing Harm**
  - Definition: ***Practices that are reasonable and necessary to prevent harm to a patient or another person***
  - Example: Clinician suspects patient is at risk of domestic abuse, and that sharing certain sensitive information via online portal could place the patient at risk of harm
- **2. Promoting Security of EHI**
  - Definition: ***Permit actors to engage in practices that are reasonable and necessary to promote the security of EHI.***
  - Example: Health IT company becomes aware of a security threat may justify suspension of access to EHI for a limited time

7 Exceptions, continued

- **3. Promoting the Privacy of EHI**:
  - Definition: ***Protect the privacy of an individual's EHI.***
- **State and federal law**
  - Example: A state's law requires that a patient provide consent before her EHI can be exchanged to another covered entity, even though this isn't required by HIPAA
- **Not covered by HIPAA**
  - Example: Direct-to-consumer health IT chooses not to provide access to EHI on the basis that it could not verify the identify of the individual requesting the EHI due to reasonable and necessary privacy-protective practices
- **Denying an individual's request for access**
  - Example: An individual is denied access to the psychotherapy notes of their mental health provider
- **Not providing access pursuant to an individual's request**
  - Example: An individual submits a request to not disclose her EHI. Once this request is made, the preference stands and doesn't have to be re-submitted every year.

ONC: Other proposals

- **US Core Data for Interoperability (USCDI) – new/required data elements**
  - Provenance
  - Clinical notes
  - Pediatric vital signs
  - Address & phone number
- **Conditions of maintenance and certification**
  - Information blocking
  - Application Programming Interfaces (APIs)
- **EHI export**
  - Require health IT developers to provide the capability to electronically export all EHI in a computable format
- **Health IT for pediatric settings**
  - Recommendations for voluntary certification of health IT for pediatric care
- **Requests for Information:**
  - Opioid Use Disorder prevention and treatment
  - Patient matching
  - Exchange with registries

Consumer priorities

- **Consumer-directed exchange (via APIs) as a complement to provider-to-provider exchange – NOT a replacement**
- **Information access and sharing as a means to meaningful partnerships**
  - Not consumer "super shoppers"
- **Additional guardrails for API-enabled access**
- **Education and enforcement of information blocking proposals**
- **Whether, how to include price information within the scope of EHI**

Next steps / consumer response

- **Questions, thoughts, reactions?**
- **Comments are due Friday, May 03**
- **Organizational plans for comment?**

For more information

Contact us:

Katie Martin
Vice President
kmartin@nationalpartnership.org

Erin Mackay
Associate Director, Health IT Programs
emackay@nationalpartnership.org

Dani Gillespie
Program Assistant
dgillespie@nationalpartnership.org

Follow us:

www.facebook.com/nationalpartnership
www.twitter.com/npwf

Find us:

national partnership for women & families

www.NationalPartnership.org

1. Preventing Harm

- **"Practices that are reasonable and necessary to prevent harm to a patient or another person"**
- **Rationale:** Acknowledge 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).
- **Example:**
  - Clinician suspects patient is at risk of domestic abuse, and that sharing certain sensitive information via online portal could place the patient at risk of harm

2. Promoting the Security of EHI

- **"Permit actors to engage in practices that are reasonable and necessary to promote the security of EHI"**
- **Rationale:** Protect practices that directly relate to protecting the security of EHI
- Note: If an actor cannot deny an individual's request to share their data with a third party, even if they disagree with the worthiness of the recipient or have concerns about what the third party might do with the EHI
- Example:
  - Awareness of a security threat may justify suspension of access to EHI, but only for the period which the threat persists. If access is denied to cohorts to which the threat does not apply, or longer than the risk persists, this would be considered information blocking

3. Promoting the Privacy of EHI

- **"Protect the privacy of an individual's EHI. Provided certain conditions are met.**
- **Rationale:** Support basic trust and confidence in health IT infrastructure
- **To be covered by this exception, you MUST qualify for at least one of the following sub-exceptions:**
  - (1) State or federal law
  - (2) Not covered by HIPAA Privacy Rule
  - (3) Denying an individual's request for access
  - (4) Not providing access pursuant to an individual's request

4. Recovering Costs Reasonably Incurred

- **"The recovery of certain costs reasonably incurred to provide access, exchange, or use of EHI."**
- **Rationale:** Enable actors to recover costs that they reasonably incur and create incentives to invest in, develop, and disseminate interoperable technologies
- **Example:**
  - "Reasonable" fees for access, such as when EHI is provided on paper copies or CD/flash drive are included in this exception, however a fee for electronic access or a consumer-authorized third party app would be considered information blocking

5. Responding to Infeasible Requests

- **"Permit an actor to decline the provide access, exchange or use of EHI in a manner that is infeasible, provided certain conditions are met"**
- **Rationale:** 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.
  - Trying to accommodate infeasible requests may result in disruption to health care operations or solutions that are financially unsustainable.
  - Note: "burdens" cannot include factors that will get in the way of the actor's pursuit of economic advantage, such as its ability to charge higher prices or capture a market share.
- **Example:** A small physician practice with limited financial and technical resources may find it burdensome to accommodate requests that a large health system with a large IT department may be able to accommodate.

6. Licensing Interoperability Requirements

- **"Actors are permitted to license interoperability elements on a reasonable and non-discriminatory terms"**
- **Rationale:** 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.
- **Example**:
  - An actor licenses a technology to a competitor and charges a royalty for the technology that is consistent and not based on strategic value to the actor of controlling the technology
  - It IS information blocking if an actor offers a license to a competitor at a royalty rate significantly higher than was offered to a party not in direct competition with the actor

7. Maintaining and Improving health IT Performance

- **"Practices that are reasonable and necessary to maintain and improve the overall performance of health IT"**
- **Rationale:** recognize 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.
- **Example:** a large health system takes its system offline for four hours each month to conduct routine maintenance