Meeting Notes

Health Information Technology Advisory Committee
February 20, 2019, 09:30 a.m. – 01:00 p.m. ET
Virtual

The February 20, 2019, meeting of the Health IT Advisory Committee (HITAC) was opened at 9:30 a.m. ET by **Lauren Richie**, Designated Federal Officer (DFO), Office of the National Coordinator for Health IT (ONC).

Lauren Richie reminded the HITAC members to use the hand raising feature in Adobe when asking a question. If a member is on the phone only, she welcomed them to speak up to be put into the queue. She then conducted roll call.

Roll Call

MEMBERS IN ATTENDANCE

Carolyn Petersen, Individual, Co-chair
Robert Wah, DXC Technology, Co-chair
Michael Adcock, University of Mississippi Medical Center
Christina Caraballo, Audacious Inquiry
Tina Esposito, Advocate Health Care
Cynthia A. Fisher, WaterRev, LLC
Brad Gescheider, PatientsLikeMe
Valerie Grey, New York eHealth Collaborative
Anil Jain, IBM Watson Health Kensaku Kawamoto, University of Utah Health
John Kansky, Indiana Health Information Exchange
Steven Lane, Sutter Health
Leslie Lenert, Medical University of South Carolina
Clem McDonald, National Library of Medicine
Arien Malec, Change Healthcare
Denni McColm, Citizens Memorial Healthcare
Aaron Miri, The University of Texas at Austin, Dell Medical School and UT Health Austin
Brett Oliver, Baptist Health
Terrence O'Malley, Massachusetts General Hospital
Raj Ratwani, MedStar Health
Steve L. Ready, Norton Healthcare
Sasha TerMaat, Epic
Andrew Truscott, Accenture LLP
Sheryl Turney, Anthem BCBS
Denise Webb, Marshfield Clinic Health System

MEMBERS NOT IN ATTENDANCE

Kate Goodrich, Centers for Medicare & Medicaid Services (CMS)

Chesley Richards (CDC)
Patrick Soon-Shiong, NantHealth
Ram Sriram, National Institute of Standards and Technology (NIST)

ONC STAFF

Donald Rucker, National Coordinator
Steve Posnack, Executive Director, Office of Technology
Elise Sweeney Anthony, Executive Director, Office of Policy
Seth Pazinski, Director, Division of Strategic Planning and Coordination
Michael Lipinski, Director, Division of Regulatory Affairs
Lauren Richie, Designated Federal Officer

Call to Order

Lauren Richie called the meeting to order and turned the meeting over to the Donald Rucker, National Coordinator.

Welcome Remarks

Donald Rucker, National Coordinator, shared that this is an important meeting to review the 21st Century Cures Act (Cures): Interoperability, Information Blocking, and the ONC Health IT Certification Program Notice of Proposed Rule Making (NPRM) that was released on February 11, 2019. The proposed rule implements the provisions around seamless and secure access exchange and use of electronic health information, as required in Cures. He looks forward to receiving the HITAC's input and feedback on the NPRM. Some specifics of the NPRM include requiring standards-based application programming interfaces (APIs) and identification of exceptions to the prohibition of information blocking. There will be a review of some of the certification steps needed. There also is a request for information regarding what additional information would be needed for price transparency, which is a national issue that comes up with patient access and control. The NPRM maps almost exactly to what Congress had as the three priorities for HITAC including interoperability, privacy and security, and patient access.

He noted that the draft trusted exchange framework is forthcoming. He also shared that the Strategy on Reducing Burden Relating to the Use of Health IT and EHRs identified prior authorization as an issue and there may be some opportunities to do work there in the future. He thanked the members in advance for their work on the NPRM and transitioned to Alex Mugge from the Centers for Medicare & Medicaid Services (CMS) to talk about the companion proposed rule.

Alex Mugge, Deputy Chief Informatics Officer, CMS provided an update on the Interoperability and Patient Access Proposed Rule. She noted that there is a slightly different approach to interoperability in the ONC and CMS rules, but both have the same end goal. The CMS rule has policies for health plans, clinicians, hospitals, and post-acute care providers. CMS worked closely with ONC on the development of the rule which is demonstrated in the way that the ONC and CMS rules complement one another. Both rules have adopted the fast healthcare interoperability resources (FHIR) standards for interoperability to

support seamless data exchange. There is a proposal for information blocking within the CMS rule to demonstrate the Department of Health and Human Service's commitment to stop information blocking.

She encouraged the HITAC members to follow-up with additional questions.

Lauren Richie transitioned to the HITAC co-chairs.

Review of Agenda and Approval of December Meeting Minutes

Carolyn Petersen, HITAC co-chair, reviewed the agenda. She shared that there will be a review of the NPRM and the proposed HITAC task forces assigned to review the rule. There will also be a review of the draft annual report.

Carolyn Petersen called for a vote to approve the minutes from the December 13, 2018 meeting. No comments or amendments were offered; the minutes were approved.

Robert Wah, co-chair, thanked the HITAC members for their patience with the changes to recent meetings due to the government shut-down in late 2018.

Lauren Richie transitioned to Elise Sweeney Anthony.

21st Century Cures Proposed Rule Overview and Task Force Establishment

IMPLEMENTATION OF THE 21ST CENTURY CURES ACT
Elise Sweeney Anthony, Executive Director, Office of Policy, ONC

Elise Sweeney Anthony noted that the NPRM includes many policies that ONC has been thinking through and there is a lot that will be presented. She shared that the same presentation was used at HIMSS. She noted that public comments need to be submitted through the public comment process. The NPRM is posted on the ONC website. It is not yet posted to the federal registered, once posted, the 60-day comment period will begin. She also shared that there are fact sheets posted on the website to help digest the NPRM.

She noted that Michael Lipinski will review the HITAC task forces that will be charged with reviewing the NPRM and providing comments. There will be time to dive deeper into specific NPRM questions during the task force meetings.

Sec. 4001 Pediatrics

- ONC developed ten recommendations for the voluntary certification of health IT for pediatric care in response to the requirement set forth by Congress in Section 4001 of the Cures Act.
- ONC proposes to adopt new and revised certification criteria to support the voluntary certification of health IT for use by pediatric health providers to support the health care of children.

- ONC is also focused on non-regulatory initiatives that are nimble and responsive to stakeholders, including development of informational resources to support setting-specific implementation that aligns with the ONC Health IT Certification Program.

Sec. 4002 Conditions of Certification

- ONC proposes an approach whereby the Conditions and Maintenance of Certification express initial and ongoing requirements for health IT developers and their certified Health IT Modules.
- The Conditions of Certification with accompanying Maintenance of Certification requirements, consistent with the Cures Act, would focus on: (a) information blocking; (b) assurances; (c) communications; (d) application programming interfaces (APIs); (e) real world testing of certified health IT; and (f) attestations.
- ONC proposes an enforcement approach to encourage consistent compliance with the requirements. The proposed rule outlines a corrective action process for ONC to review and act for potential or known instances where a Condition or Maintenance of Certification requirement is not being met by a health IT developer under the ONC Health IT Certification Program.

Sec. 4003 Interoperability Definition

- ONC proposes that interoperability means, with respect to health IT, such health IT that: (1) enables the secure exchange of electronic health information (EHI) with, and use of EHI from, other health IT without special effort on the part of the user; (2) allows for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable state or federal law; and (3) does not constitute information blocking.
- The proposed definition is consistent with the Cures Act interoperability definition.

Sec. 4004 Information Blocking

- ONC proposes seven categories of practices that would be considered reasonable and necessary that, provided certain conditions are met, would not constitute information blocking. These categories were developed based on feedback from stakeholders and consultation with appropriate federal agencies.
- If the actions of a regulated actor (health care provider, health IT developer, or health information exchange or network) satisfy an exception, the actions would not be treated as information blocking, and the actor would not be, as applicable, subject to civil penalties or other disincentives under the law.

Sec. 4005 Exchange with Registries

- ONC's proposed rule includes a Request for Information (RFI) on how a standards-based API might support improved information exchange between a health care provider and a registry in support of public health reporting, quality reporting, and care quality improvement.
- Public input on this RFI may be considered for future HHS rulemaking to support the bidirectional exchange of clinical data between health care providers and registries for a wide range of use cases.

Sec. 4006 Patient Access

- ONC proposes to promote policies that would ensure a patient's EHI is accessible to that patient and the patient's designees, in a manner that facilitates communication with the patient's health care providers and other individuals, including researchers, consistent with such patient's consent through the following proposals: United States Core Data for Interoperability (USCDI) standard; "EHI export" criterion; "standardized API for patient and population services" criterion, "data segmentation for privacy (DS4P)" criteria, "consent management for APIs" criterion; API Condition of Certification; and information blocking requirements, which include providing patients access to their EHI at no cost to them.
- Patient access to their EHI would be improved through the adoption of the following proposed 2015 Edition standard and certification criteria: USCDI standard; standardized APIs for patient and population services; and EHI export.

Implementation of Executive Orders

Executive Order 13813 Promoting Healthcare Choice and Competition Across the United States

- ONC's proposed rule would contribute to fulfilling Executive Order 13813 by furthering patient (and health care provider) access to EHI and supporting competition in health care markets through new tools to access EHI and policies to address the hoarding of EHI.
- ONC's proposed rule calls on the health care industry to adopt standardized APIs, which would allow individuals to securely and easily access structured EHI using new and innovative applications for smartphones and other mobile devices.
- The proposed rule would establish information blocking provisions, focusing on improving patient and health care provider access, exchange, and use of EHI.

Executive Orders 13771 & 13777 Reducing Regulation and Controlling Regulatory Costs and Enforcing the Regulatory Reform Agenda

- ONC reviewed and evaluated existing regulations to identify ways to reduce burden and implement deregulatory actions.
- ONC proposes potential deregulatory actions that will reduce burden for health IT developers, providers, and other stakeholders. These six deregulatory actions are: (1) removal of a threshold requirement related to randomized surveillance; (2) removal of the 2014 Edition from the Code of Federal Regulations (CFR); (3) removal of the ONC Approved Accreditor (ONC-AA) from the Certification Program; (4) removal of certain 2015 Edition certification criteria; (5) removal of certain Certification Program requirements; and (6) recognition of relevant Food and Drug Administration (FDA) certification processes with a request for information on the potential development of new processes for the ONC Health IT Certification Program.

Purpose

- Increase Innovation and Competition
    - by giving patients and their health care providers safe and secure access to health information and to new tools, allowing for more choice in care and treatment.
- Reduce Burden and Advance Interoperability

  - using the United States Core Data for Interoperability (USCDI) standard, new API requirements, and EHI export capabilities for the purposes of switching health IT or to provide patients their electronic health information.
- Promote Patient Access
  - through a provision requiring that patients can electronically access all their electronic health information (structured and/or unstructured) at no cost.

UPDATES TO THE 2015 EDITION CERTIFICATION
Michael Lipinski, Division Director, Regulatory Affairs, ONC

Michael Lipinski thanked the HITAC for the opportunity to share the details of the rule. He noted that the rule has been a labor of love and he is excited to share it with the public and hear comments. He reiterated that any changes that may occur between now and when the rule will be posted on the Federal Register will only be formatting changes. Once displayed, it will be published, and the 60-day comment period will start. He shared that ONC is trying to implement the 21st Century Act in a way that achieves the purpose of increasing innovation, competition, reducing burden, advancing interoperability, and promoting patient access.

Proposed Changes to the 2015 Edition Certification Criteria

- Removed some items because they have been implemented since the 2011 edition or the functionality has been in the certification program for some time and it is unlikely that developers will remove them.
- Items removed include:
  - Problem list (§ 170.315(a)(6))
  - Medication list (§ 170.315(a)(7))
  - Medication allergy list (§ 170.315(a)(8))
  - Smoking status (§ 170.315(a) (11))
  - Drug formulary and preferred drug list checks (§ 170.315(a) (10)
  - Patient-specific education resource (§ 170.315(a) (13))
  - 2015 Base EHR Definition Criteria Other Criteria
  - Common Clinical Data Set summary record – create (§ 170.315(b)(4))
  - Common Clinical Data Set summary record – receive (§ 170.315(b)(5))
  - Secure messaging (§ 170.315(e)(2))
- Updated items are captured in the table below:

Remove	Update with
Electronic prescribing (§ 170.315(b)(3))	Electronic prescribing (§ 170.315(b)(11))
Data export (§ 170.315(b)(6))	Electronic health information (EHI) export (§ 170.315(b)(10))
Data segmentation for privacy – send (§ 170.315(b)(7))	Data segmentation for privacy – receive (§ 170.315(b)(13))

Application access – data category request (§ 170.315(g)(8))	Standardized API for patient and population services (§ 170.315(g)(10))

- Revised Criteria
  - Clinical Quality Measures (CQMs) – report criterion (§ 170.315(c)(3))
- New Criteria
  - Consent management for application programming interfaces § 170.315(g)(11)
  - Encrypt authentication credentials certification criterion § 170.315(d)(12)
  - Multi-factor authentication (MFA) criterion § 170.315(d)(13)

The United States Core Data for Interoperability Standard (USCDI)

- Builds on the common clinical data set (CCDS)
- Added new data classes and elements
  - Provenance
  - Clinical notes
  - Pediatric vital signs
  - Patient address and phone number
  - There will be a task force focused on USCDI

Electronic Health Information (EHI) Export Criterion

- Functionality to support patient access and the exchange of information, and spur innovation
- Two use cases
  - Provider who wants to change their electronic health record (EHR) or HIT vendor
  - If a patient asks for their electronic data
- The data dictionary needs to be available to pull data out
- A fee cannot be charged with pulling data out

Application Programming Interface (API) Criterion

- Replacing APIs which currently don't have a standard
- There are options within the rule around which version of FHIR should be adopted
- Supports two types of API-enabled services
  - Services for which a single patient's data is the focus
  - Services for which multiple patients' data are the focus Two use cases are to get single and multiple patient data
- This will reduce burden, improve care coordination, and promote competition
- Steve Posnack will discuss further

Conditions and Maintenance of Certification

- There are seven conditions of maintenance of certification; this rule will layout six of them
  1. Information Blocking
  2. Assurances
  3. Communications
  4. Application Programming Interfaces (APIs)

5. Real World Testing
6. Attestations
7. (Future) Electronic Health Record (EHR) Reporting Criteria Submission

Information Blocking - § 170.401

- Condition required to confirm that develops will not information block, this will need to be attested to

Assurances - § 170.402

- Developers have to provide further assurances to the Secretary that will inhibit the exchange and use of EHI
- Looking at the business behaviors of the developer
- Conditions of Certification
    1. Full Compliance and Unrestricted Implementation of Certification Criteria Capabilities
    2. Certification to the "Electronic Health Information (EHI) Export" Criterion
    3. Records and Information Retention
        - Records support functionality, product does what it says it can do
    4. Trusted Exchange Framework and the Common Agreement (TEFCA) - Request for Information

Communications - § 170.403

- Implementing a statutory provision. Developers should not prohibit communication
- Requires that a health IT developer does not prohibit or restrict communication regarding the following subjects for the health IT:
    - Usability
    - Interoperability
    - Security
    - User experiences
    - Business practices
    - The way a user of health IT has used such technology

Application Programming Interfaces - § 170.404

- Rolled out within 24 months to all users and customers

Real World Testing - § 170.405

- Wanted to see developers test products in a live environment
- Ask providers to share a plan for testing
- There is a proposal related to standards advancement process

Standards Version Advancement Process

- Allow developers to move to new standards when available
- Approve versions 1.2 for the program; developer can move to the new version and show that they can real-world test to the new version

- This will provide assurances that this product is able to meet the new version of the criteria

Attestations - § 170.406

- Developers will be required to attest to compliance with the Conditions and Maintenance of Certification, except for the "EHR reporting criteria submission" Condition of Certification

Enforcement of the Conditions and Maintenance of Certification Requirements

Enforcement Approach

- ONC would be the sole party responsible for enforcing compliance. ONC may, however, coordinate its review with the HHS Office of Inspector General (OIG) or defer to the OIG to lead review of a claim of information blocking.
- ONC will use the processes established for ONC direct review of certified health IT in the Enhanced Oversight and Accountability (EOA) final rule for enforcement.
- Six steps:
  - Initiating Review and Health IT Developer Notice
  - Records Access
  - Corrective Action Plan
  - Certification Ban and/or Termination
  - Appeal
  - Public Listing of Certification Ban and/or Terminations

Michael Lipinski turned the discussion back to Elise Sweeney Anthony to discuss information blocking.

INFORMATION BLOCKING
Elise Sweeney Anthony, Executive Director, Office of Policy, ONC

Information Blocking Approach

- Section 4004 of the Cures Act authorizes the Secretary to identify reasonable and necessary activities that do not constitute information blocking.
- "Actors" regulated by the information blocking provision:
  - Health Care Providers
  - Health IT Developers of Certified Health IT
  - Health Information Exchanges
  - Health Information Networks
- In consultation with stakeholders, ONC has identified seven categories of practices that would be reasonable and necessary, provided certain conditions are met.
  - Defined through the exceptions proposed at 45 CFR 171.201–207
- If the actions of a regulated actor 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.

Key Concepts

- What is information blocking?
  - A practice by a health care provider, health IT developer, health information exchange, or health information network 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.
- Electronic Health Information (EHI)
  - ONC proposes to define EHI to mean electronic protected health information (as defined in HIPAA), and any other information that:
    - is transmitted by or maintained in electronic media (as defined in 45 CFR 160.103);
    - identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual;
    - 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 that is created or received by a health care provider.
  - Does not include health information that is de-identified consistent with the requirements of 45 CFR 164.514(b).

Price Information – Request for Information

- The fragmented and complex nature of pricing within the health care system has decreased the efficiency of the health care system and has had negative impacts on patients, health care providers, health systems, plans, plan sponsors and other key health care stakeholders.
- Consistent with its statutory authority, the Department is considering subsequent rulemaking to expand access to price information for the public, prospective patients, plan sponsors, and health care providers.
- ONC has a unique role in setting the stage for such future actions by establishing the framework to prevent the blocking of price information.
  - ONC seeks comment on the parameters and implications of including price information within the scope of EHI for purposes of information blocking.
  - The overall Department seeks comment on the technical, operational, legal, cultural, environmental and other challenges to creating price transparency within health care.

Information Blocking Exceptions

- ONC is hoping to identify whether the exceptions strike the appropriate balance.
- § 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.
- § 171.202 Exception | Promoting the Privacy of Electronic Health Information
  - An actor must satisfy at least one of four discrete sub-exceptions that address scenarios that recognize existing privacy laws and privacy-protective practices:

        - practices that satisfy preconditions prescribed by privacy laws;
        - certain practices not regulated by HIPAA but which implement documented and transparent privacy policies;
        - denial of access practices that are specifically permitted under HIPAA;
        - practices that give effect to an individual's privacy preferences.
- § 171.203 Exception | Promoting the Security of Electronic Health Information
    - 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.
- § 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:
        - charged based on objective and verifiable criteria uniformly applied to all similarly situated persons and requests;
        - related to the costs of providing access, exchange, or use; and
        - 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.
- § 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 (considering the cost to the actor, actor's resources, etc.).
    - The actor must timely respond to infeasible requests and work with requestors to provide a reasonable alternative means of accessing the 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.

- 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.
  - The practice must be implemented in a consistent and non-discriminatory manner.
  - 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.

Complaint Process and Requests for Information

Complaint Process

- Section 3022(d)(3)(A) of the PHSA directs the National Coordinator to implement a standardized process for the public to submit reports on claims of health information blocking.
- ONC intends to implement and evolve this complaint process by building on existing mechanisms, including the complaint process currently available at https://www.healthit.gov/healthit-feedback.
- ONC requests comment on this approach and any alternative approaches that would best effectuate this aspect of the Cures Act.

Additional Exceptions

- ONC is considering whether to propose, in a future rulemaking, a narrow exception to the information blocking provision for practices that are necessary to comply with the requirements of the Common Agreement.
- ONC welcomes comment on any potential new exceptions that should be considered for future rulemaking.

Disincentives for Health Care Providers

- ONC requests information on disincentives or if modifying disincentives already available under existing HHS programs and regulations would provide for more effective deterrents.

Health IT for Pediatric Care and Practice Settings

Health IT for Pediatric Care and Practice Settings

- In response to the requirements set forth in section 4001 of the Cures Act, ONC has:
  1. Developed ten recommendations for the voluntary certification of health IT for pediatric care that does NOT include a separate certification program for pediatric care and practice settings.
  2. Identified current and proposed new 2015 Edition certification criteria that support pediatric care and practice settings.
  3. Focused on non-regulatory initiatives that are nimble and responsive to stakeholders, including development of informational resources to support setting-specific implementation that aligns with the ONC Health IT Certification Program.

ONC Developed Recommendations Based on Stakeholder-Identified Clinical Priorities and the Children's EHR Format – for Voluntary Certification Criteria

1. Use biometric-specific norms for growth curves and support growth charts for children

2. Compute weight-based drug dosage
3. Ability to document all guardians and caregivers
4. Segmented access to information
5. Synchronize immunization histories with registries
6. Age- and weight-specific single dose range checking
7. Transferrable access authority
8. Associate mother's demographics with a newborn
9. Track incomplete preventative care opportunities
10. Flag special health care needs

Proposed New 2015 Edition Criteria

- United States Core Data Set for Interoperability (USCDI)
- Electronic prescribing
- FHIR-based API
- Data segmentation for privacy

Additional Requests for Information (RFIs)

Health IT and Opioid Use Disorder Prevention and Treatment RFI

- ONC recognizes that health IT offers promising strategies to help medical specialties and sites of service as they combat opioid use disorder (OUD).
- ONC requests public comment on how our existing Program requirements and the proposals in this rulemaking may support use cases related to opioid use disorder (OUD) prevention and treatment and if there are additional areas that ONC should consider for effective implementation of health IT to help address OUD prevention and treatment.

Patient Matching RFI

- Patient matching is a critical component to interoperability and the nation's health information technology infrastructure. Accurate patient matching helps health care providers access and share the right information on the right patient when and where it is needed.
- Section 4007 of the 21st Century Cures Act directed the Government Accountability Office (GAO) to conduct a study on patient matching.
    - The GAO report, Approaches and Challenges to Electronically Matching Patients' Records across Providers, was released in January 2019. https://www.gao.gov/assets/700/696426.pdf
- ONC seeks comment on additional opportunities that may exist in the patient matching space and ways that ONC can lead and contribute to coordination efforts with respect to patient matching. ONC and CMS collaborated to jointly issue complementary requests for information regarding patient matching.

Exchange with Registries

- Section 4005 (a) and (b) of the Cures Act focuses on interoperability and bidirectional exchange between EHRs and registries, including clinician-led clinical data registries. ONC is approaching these provisions from several angles to address the technical capability of EHRs to exchange data with registries in accordance with applicable recognized standards.

- ONC included an RFI in the proposed rule on how a standards-based API might support improved information exchange between a health care provider and a registry to support public health reporting, quality reporting, and care quality improvement. Public input on this RFI may be considered for future HHS rulemaking to support the bidirectional exchange of clinical data between health care providers and registries for a wide range of use cases.

21st Century Cures Act NPRM – Regulatory Implementation Milestones

- From the effective date of the final rule, there will be a two-year timeframe of when these items need to be in place.

Discussion

- **Denise Webb** expressed concern regarding the 60-day review period. She asked if there as an ability to extend the review period, several CIOs have expressed concern about the timing.
  - **Elise Sweeney Anthony** shared that ONC is planning to keep a 60-day comment period. She did note that the NPRM has been out for over a week and the clock has not yet started because it hasn't been posted in the Federal Register.
- **Arien Malec** questioned the definition of "provider" from the Public Health Service Act. He thought it would be helpful to clarify what is included in the definition of "provider".
  - **Michael Lipinski** shared that the definition is also specified in Cures. The provider term is broad and includes hospital, nursing facility, home health entity, healthcare clinic, community mental health central, renal dialysis, ambulatory surgical center, pharmacy, laboratory, physician, tribal organizations, rural health clinics, and any other category of health care facility, entity, practitioner, or clinician determined appropriate by the Secretary. ONC would appreciate comments on the definition.

API CONDITIONS OF CERTIFICATION

Steve Posnack, Executive Director, Office of Technology, ONC

Big Picture Scope and Applicability: Certified-API Proposals

- Information Blocking
  - Applies to health IT developers, health information exchanges, health information networks, and health care provider
  - Electronic health information is expected to be accessible, exchangeable, & useable unless an "interference" is required by law or covered by an exception(s)
  - An action(s) covered by an exception(s) would not be subject to penalties or disincentives
- API Conditions of Certification
  - Three specific conditions:
    - Transparency Condition
    - Permitted Fees Condition
    - Openness and Pro-Competitive Conditions
    - Maintenance of Certification Requirements
- API Certification Criteria

- New 2015 Edition "Cures Criterion"
  - Secure, standards-based API (170.315(g) (10)) - "read-only" focus
  - HL7® FHIR® as base standard
  - Other implementation specifications to (e.g., SMART App Launch Framework + OAuth 2 + OpenID Connect 1.0) to support for provider and patient-access use cases

API Conditions of Certification

- Who?
  - API Technology Supplier: Health IT developer of certified API technology
  - API Data Provider: Health care organization that deploys the API technology
  - API User: Persons and entities that use or create software applications (e.g., third party services, health care organization itself) that interact with API technology API Conditions of Certification
- What?
  - Applies to all API-focused certification criteria (170.315(g)(7) through proposed (g) (10) and (11))
  - Practically speaking "FHIR Servers"
- How?
  - The API Condition of Certification applies only to health IT developers and health IT that is certified to any of the API-focused certification criteria

New API Certification Criteria 170.315(g) (10) to replace (g)(8) Standards-based API for patient and population services

- Required Capability(ies)
  - App registration
  - Secure connection
  - 1st time Authentication & App Authorization + (get refresh token)
  - Data response
  - Search
  - Subsequent Authentication & App Authorization + (new refresh token)
  - Documentation
- Applicable Standard(s)
  - None; Dynamic Registration permitted
  - SMART Application Launch Framework IG
  - OpenID Connect + SMART Application Launch Framework IG
  - FHIR (Release 2) + (API Resource Collection in Health) ARCH + Argonaut Data Query IG Profiles
  - Argonaut Data Query IG Server
  - SMART Application Launch Framework IG
  - None; Must be made publicly accessible
- Additional Context
  - Associated API CoC
  - Must support patient and clinical- access
  - Must support access to a single patient's data & data for multiple patients

- Must support “Standalone Launch” and “EHR Launch.”
- Refresh tokens with a lifetime of at least 3 months
- Associated API CoC

FHIR Server Testing

- Inferno is an open source tool that tests whether patients can access their health data. It makes HTTP(S) requests to test your server's conformance to authentication, authorization, and FHIR content standards and reports the results back.

FHIR Implementation Nationwide

- A blog post was released last fall discussing FHIR implementation nationwide and shared during a previous HITAC meeting.
- Of the hospitals and Merit-based Incentive Payment System (MIPS) eligible clinicians that use certified products, ONC found that almost:
  - 87% of hospitals and 69% of MIPS eligible clinicians are served by health IT developers with product(s) certified to any FHIR version.

The US Core Data for Interoperability (USCDI v1)

- Steve shared all the items included
- ONC proposes to have updates and have a process in place for updating moving forward

Translating the USCDI into Computable Content

- Needs to be translated to a language in FHIR
- Applicable FHIR Resources were selected to support USCDI Data Classes and Data Elements

What is the API Resource Collection in Health (ARCH)?

- 15 Specific FHIR Resources aligned to support the USCDI
- Referenced in new 170.315(g)(10) certification criterion
- Use existing specifications to add profile clarity to resources

API Conditions and Maintenance of Certification High-level Overview

- Cures Act Condition
  - An API Technology Supplier must publish APIs and must allow health information from such technology to be accessed, exchanged, and used without special effort using APIs or successor technology or standards, as provided for under applicable law, including providing access to all data elements of a patient’s electronic health record to the extent permissible under applicable privacy laws
- Transparency
  - Publicly accessible documentation
  - Terms and conditions
  - Fees and structure
  - App developer verification process
- Permitted Fees
  - Only specific types of fees are permitted

    - Must have objective and verifiable criteria
    - Three categories of permitted fees
    - Must keep detailed records for fees
- Openness and Pro-competitive
    - Must grant API Data Providers sole authority
    - Terms must be non-discriminatory
    - All necessary "rights" must be provided
    - Must maintain service and support levels
- Maintenance of Certification
    - An API Technology Supplier must register and enable apps for production use within one business day of completing its verification of an app developer's authenticity.
    - An API Technology Supplier must support the publication of Service Base URLs (i.e., FHIR API endpoints) for all its customers and make such information publicly available (in a computable format) at no charge.
    - An API Technology Supplier with API technology previously certified to § 170.315(g)(8) must provide all API Data Providers with a (g) (10)-certified API within 24 months of a final rule's effective date.

The API Conditions of Certification Transparency Conditions

- The business and technical documentation published by an API Technology Supplier must be complete. All documentation must be published via a publicly accessible hyperlink that allows any person to directly access the information without any preconditions or additional steps.
    - The API Technology Supplier must publish all terms and conditions for its API technology.
    - Any and all fees charged by an API Technology Supplier for the use of its API technology must be described in detailed, plain language.
    - An API Technology Supplier is permitted to institute a process to verify the authenticity of application developers.

The API Conditions of Certification & Information Blocking Permitted Fees

- The API Technology Supplier is the actor that is regulated by the API Conditions of Certification.
- Information Blocking has a larger umbrella of actors
    - Two different types of relationships:
        - Customers
        - Direct relationships with user
- Permitted fees have three categories:
    - Go beyond information blocking exception
    - Development, deployment, and upgrade
    - API usage costs incurred by the supplier when providing services on an ongoing basis

The API Conditions of Certification Permitted Fees: General Conditions

- The industry is asked to provide additional areas of for fees, if deemed necessary.
- All fees related to API technology not otherwise permitted are prohibited from being imposed by an API Technology Supplier.
- For all permitted fees, an API Technology Supplier must:

- Ensure that fees are based on objective and verifiable criteria that are uniformly applied
- Ensure that fees imposed on API Data Providers are reasonably related to the API Technology Supplier's costs of supplying
- Ensure that the costs of supplying and, if applicable, supporting the API technology upon which the fee is based are reasonably allocated among all customers
- Ensure that fees are not based in any part on whether the requestor or other person is a competitor

Scenario #1, Permitted Fee #1 Development, Deployment, and Upgrade Fees

- An API Technology Supplier is permitted to charge fees to an API Data Provider to recover the costs reasonably incurred by the API Technology Supplier to develop, deploy, and upgrade API technology for the API Data Provider.
- An API Technology Supplier is NOT permitted to establish "relationship" fees between itself and an API User just because of the API User's connectivity to or mutual business relationship with the API Technology Supplier's customer (i.e., the API Data Provider).

Scenario #1, Permitted Fee #2 API Usage Costs

- An API Technology Supplier is permitted to charge fees to an API Data Provider to recover the incremental costs reasonably incurred by the API Technology Supplier to support the use of API technology deployed by or on behalf of the API Data Provider.
- An API Technology Supplier is only permitted to charge the API Data Provider. If an API User exceeds service established levels, the API Data Provider would be responsible for paying the extra charges.
- If an API Data Provider administers the API on its own (i.e., assumes full responsibility), then API Technology Supplier would not be permitted to charge usage fees.
- The costs recovered under "usage-based" fees would only be able to reflect "post-deployment" costs.
- No fee amount, threshold, or methodology is proposed. It is up to the API Technology Supplier to determine consistent with the "general conditions" and information blocking.
- This permitted fee DOES NOT include:
  - Any costs incurred by the API Technology Supplier to support uses of the API technology that facilitate a patient's ability to access, exchange, or use their electronic health information.
  - Costs associated with intangible assets (including depreciation or loss of value), except the actual development or acquisition costs of such assets. o Opportunity costs, except for the reasonable forward-looking cost of capital.
  - (reiterated) An API Technology Supplier is NOT permitted to establish "relationship" fees between itself and an API User just because of the API User's connectivity to or mutual business relationship with the API Technology Supplier's customer (i.e., the API Data Provider).

Scenario #2, Permitted Fee #3 Value Added Services Fees

- An API Technology Supplier is permitted to charge fees to an API User for value-added services supplied in connection with software that can interact with the API technology, provided that

such services are not necessary to efficiently and effectively develop and deploy such software (i.e., production-ready software).

- Permits API Technology Suppliers to offer market differentiating services that could make it attractive for API Users to develop software applications that can interact with the API technology. • Examples: advanced training, premium development tools and distribution channels, enhanced compatibility/integration testing assessments, co-branded integration, co-marketing arrangements, promoted placement in "app store."
- API Technology Suppliers would be able to administer their own "app stores" if they do not violate this condition of certification and information blocking policies.
- For example, if a software developer's app were required to go through a paid listing process as a precondition to be able to be deployed (and generally accessible) to the API Technology Supplier's health care provider customers to use, this would not be a permitted fee under this Condition of Certification, would constitute special effort, and could raise information blocking concerns.

The API Conditions of Certification Openness and Pro-Competitive Conditions (1)

- An API Technology Supplier must grant an API Data Provider the sole authority and autonomy to permit API Users to interact with the API technology deployed by the API Data Provider.
- Non-Discriminatory Terms
    - An API Technology Supplier must provide API technology to API Data Providers on terms that are no less favorable than it provides to itself
    - The terms on which an API Technology Supplier provides API technology must be based on objective and verifiable criteria
    - An API Technology Supplier must not offer different terms or service based on:
        1. Whether the API User with whom an API Data Provider has a relationship is a competitor
        2. The revenue or other value the API User with whom an API Data Provider has a relationship may derive from access, exchange, or use of electronic health information obtained by means of API technology

The API Conditions of Certification Openness and Pro-Competitive Conditions (2)

- An API Technology Supplier must grant an API Data Provider the sole authority and autonomy to permit API Users to interact with the API technology deployed by the API Data Provider.
- Rights to access and use API technology
- An API Technology Supplier must have and, upon request, must grant to API Data Providers and their API Users all rights that may be reasonably necessary to access and use API technology in a production environment, including:
    1. For the purposes of developing products or services that are designed to be interoperable with the API Technology Supplier's health information technology or with health information technology under the API Technology Supplier's control;
    2. Any marketing, offering, and distribution of interoperable products and services to potential customers and users that would be needed for the API technology to be used in a production environment; and
    3. Enabling the use of the interoperable products or services in production environments, including accessing and enabling the exchange and use of electronic health information.

- An API Technology Supplier must not condition any of the rights described on the requirement that the recipient of the rights do, or agree to do, any of the following:
    1. Pay a fee to license such rights, including but not limited to a license fee, royalty, or revenue-sharing arrangement.
    2. Not compete with the API Technology Supplier in any product, service, or market.
    3. Deal exclusively with the API Technology Supplier in any product, service, or market.
    4. Obtain additional licenses, products, or services that are not related to or can be unbundled from the API technology.
    5. License, grant, assign, or transfer any intellectual property to the API Technology Supplier.
    6. Meet additional developer or product certification requirements.
    7. Provide the API Technology Supplier or its technology with reciprocal access to application data.

The API Conditions of Certification Openness and Pro-Competitive Conditions (3)

- An API Technology Supplier must grant an API Data Provider the sole authority and autonomy to permit API Users to interact with the API technology deployed by the API Data Provider. Once the organization has received API technology, the customer can choose the services used.
- Service and Support Obligations
    1. An API Technology Supplier must provide all support and other services reasonably necessary to enable the effective development, deployment, and use of API technology by API Data Providers and their API Users in production environments.
    2. An API Technology Supplier must make reasonable efforts to maintain the compatibility of its API technology and to otherwise avoid disrupting the use of API technology in production environments.
    3. Except as exigent circumstances require, prior to making changes or updates to its API technology or to the terms and conditions thereof, an API Technology Supplier must provide notice and a reasonable opportunity for its API Data Provider customers and registered application developers to update their applications to preserve compatibility with API technology and to comply with applicable terms and conditions.

Requests for Comment

- Four options proposed for FHIR Standard(s) adoption:
    - Option 1: Just FHIR Release 2 (proposed)
    - Option 2: FHIR Release 2 and Release 3 (as either one for certification option)
    - Option 3: FHIR Release 2 and Release 4 (as either one for certification option)
    - Option 4: Just FHIR Release 4
- For the Document Reference and Provenance resources, which are currently present in the base FHIR standard, ONC requests comments on the minimum “search” parameters that would need to be supported.
- On any additional specific “permitted fees” not addressed above that API Technology Suppliers should be able to recover in order to assure a reasonable return on investment. Furthermore, ONC requests comment on whether it would be prudent to adopt specific, or more granular, cost methodologies for the calculation of the permitted fees.
- On a reasonable upper bound for Refresh Token period of use.
- On whether ONCshould require support for OAuth 2.0 Dynamic Client Registration Protocol.

HITAC TASK FORCE ESTABLISHMENT

Michael Lipinski, Director Regulatory Affairs Division

Task Force Establishment

1. Information Blocking
    - In addition to the information blocking policies, this will also include the "information blocking," "assurances," and "communications" conditions and maintenance of certification requirements as well as policies for enforcement of all the conditions and maintenance of certification requirements.
2. Conditions and Maintenance of Certification Requirements
    - This includes the "API," "real world testing," and "attestations" conditions and maintenance of certification requirements. It will also include the following: updates to the 2015 Edition health IT certification criteria; changes to the ONC Health IT Certification Program; and deregulatory actions.
3. Health IT for the Care Continuum
    - This will include ONC recommendations and policies that support pediatric care and practice settings; 2015 edition certification criteria that support multiple care and practice settings; and an "opioid" request for information.
4. U.S. Core Data for Interoperability (USCDI) Standard
    - This will focus on the draft USCDI v1 data classes and data elements and the USCDI promotion model.

Lauren Richie reviewed the timeline for the task forces to provide feedback.

- She highlighted that there is an eight-week timeline. During the fifth week, draft recommendations will be reviewed with the HITAC. Recommendations will be reviewed and finalized at the HITAC meeting during the eighth week.
- She also reminded HITAC members to identify the task forces that they would like to participate in and co-chair.

Elise Sweeny Anthony added her appreciation in advance for all the members who will participate and add contributions to the NPRM.

Donald Rucker echoed Elise's appreciation.

Discussion

There was additional time remaining after the review of the draft annual report. The remaining time was used to ask questions about the NPRM.

Ken Kawamoto commented that he noticed the API requirements were around Argonaut. Assuming that was intentional, why was Argonaut selected rather than the USCDI? Argonaut is not a public, open group. It is membership only and made up of a select number of companies and health organizations participant.

- **Steve Posnack** responded that ONC canvassed the ecosystem for the implementation guidance that would be available to support a proposal associated with FHIR release two which is where the industry is today. He shared that there is a detailed discussion in the NPRM identifying the various

FHIR standards versions that are out as a base standard and the accompanying implementation for which comment is requested. He shared that ONC identified that FHIR release three was available. If ONC were to opt to adopt this, they would also adopt the implementation guidance associated with it which would be FHIR U.S. Core release 3 version implementation guidance or profiles which are the next evolution of Argonaut. He noted that for FHIR release 2 there were the Argonaut profiles and for FHIR release three the Argonaut profiles were folded into what ONC called the U.S. FHIR Core profile. For Release 4 that was just published a month or so ago, there will be a turn of the crank to update to FHIR release 4 U.S. FHIR Core profiles that will effectively be the second evolution of the original Argonaut profiles.

  - **Ken Kawamoto** expressed concerned that Argonaut is not a public group and it is concerning because it does not allow for public comment.

- **Ken Kawamoto** also commented that it is bold and great to focus on cost only API access. It seems different from any App store model. It seems that it could reduce incentives for developers to further develop these ecosystems. It may also defer free software.
  - **Michael Lipinski** recited information that is in the proposed NPRM. There was evidence in the Congressional Report and in meetings with OIG that fees were a way to prohibit PHI sharing or information block. EHI is not a commodity that can be traded or sold by the custodians of the EHI. ONC didn't think there should be any fees associated with the access, use, and exchange of EHI. ONC provided a proper basis to recovery reasonably incurred costs and to promote innovation. It is proposed that there be a licensed intellectual property (IP). Innovation is still promoted and allows the ability to recover a cost on innovation. This is considered to determine reasonable terms for licensing. He noted this is a proposed rule and welcomes comments if there is a better way to do this.
  - **Ken Kawamoto** questioned where this worked in another industry. He expressed concern for vendors being onboard.
  - **Steve Posnack** noted that in comparison to other industries there hasn't been a law such as the Cures Act that has dictated requirements for APIs to be published and used without special effort. There are a lot of unique characteristics that are different from other industries where there is a different competitive landscape and business motivators.
  - **Michael Lipinski** noted per statue; it is required to come from the perspective that sharing should happen in all instances unless required by law not to. The goal was to provide exceptions where there would be actions that would inhibit. Wanted to be able to promote access, exchange, and use. If there are unintended consequences, he urged for there to be comments**.**
- **Ken Kawamoto** questioned if he understood the one-day verification correctly. Instead of going through the current vendor-based review process for security, it is proposed in the rule that one day later it must be available to help even if they haven't been vetted by the vendor.
  - **Steve Posnack** commented that the entire sequence of events is needed for it to make sense. The one-day item referenced is the end of the sequence. This has to do with registration. If the health IT developer is in the position of registering the apps, they have a choice. They can automatically register the app through whatever mechanism they want, and the protocol is one of those. The other choice is to institute an app developer authenticity verification process. Keeping with the special effort construct, if an API technology supplier were to have and implement this authenticity verification approach there would be up to five business days. Once complete, the one-day kicks in as part of the maintenance certification. ONC did not want there to be a time where the API technology supplier doesn't get the application

registered in a timely manner. That is the one-day referenced. Once the review is complete, the app should be in the registration listing within one day. They will have some means of dynamically registering at the time an app comes in.

Sasha TerMaat Questioned if a supplier decides not to verify application developers, or to do so automatically, is there clarity that they are not liable for consequences that might occur because of the lack of vetting?

- **Steve Posnack** noted this is an important point where feedback would be appreciated for additional clarity in the final rule. There might be additional agencies that have to provide additional clarity, as well.

Donald Rucker, National Coordinator, noted that the Office for Civil Rights will help address that question.

HITAC Annual Report Draft Review

Carolyn Petersen shared the timeline and the process the workgroup used to aggregate the draft annual report. She noted that during the March 20, 2019 meeting the HITAC will vote to approve the report.

She reviewed the membership and ONC staff who helped contribute and thanked everyone for their dedicated participation.

She initiated the discussion by walking through the scope.

Annual Report Workgroup Scope

- Overarching Scope
  - The workgroup will inform, contribute to, and review draft and final versions of the HITAC Annual Report to be submitted to the HHS Secretary and Congress each fiscal year. As part of that report, the workgroup will help track ongoing HITAC progress.
- Detailed Scope
  - Provide specific feedback on the content of the report as required by the 21st Century Cures Act including:
    - Analysis of HITAC progress related to the priority target areas
    - Assessment of health IT infrastructure and advancements in the priority target areas
    - Analysis of existing gaps in policies and resources for the priority target areas
    - Ideas for potential HITAC activities to address the identified gaps

Annual Report Workgroup Next Steps

- Next steps for FY18 report development
  1. HITAC full committee reviews report and suggests edits
  2. HITAC full committee approves revised report
  3. HITAC forwards the final report to the National Coordinator for Health IT
  4. The National Coordinator forwards final report to HHS Secretary and Congress

Draft FY18 Annual Report Outline

- Executive Summary

- Foreword and Overview
- HITAC Progress in FY18 IV. Health IT Infrastructure Landscape Analysis
- Health IT Infrastructure Gap Analysis
- Recommendations for Addressing Health IT Infrastructure Gaps
- Suggestions for Additional HITAC Initiatives VIII. Conclusion IX. Appendices

Overview: HITAC Priority Target Areas

- HITAC Priority Target Areas noted in Section 4003 of the 21st Century Cures Act covers the following areas:
- Interoperability
    - Achieving a health information technology infrastructure that allows for the electronic access, exchange, and use of health information.
- Patient Access
    - The facilitation of secure access by an individual and their caregiver(s) to such individual's protected health information.
- Privacy and Security
    - The promotion and protection of privacy and security of health information in health IT.
- Any other target area
    - Related to the above target areas that the HITAC identifies as an appropriate target area to be considered on a temporary basis with adequate notice to Congress.

Carolyn Petersen then turned the review over to **Aaron Miri** to review the progress for fiscal year (FY) 2018.

HITAC Progress in FY18

- Seven HITAC meetings
- Policy Framework
- Accomplishments of Subcommittees
    - Trusted Exchange Framework Task Force
        - Nine Meeting
        - 26 recommendations
    - U.S. Core Data for Interoperability Task Force
        - Nine meetings
        - Nine recommendations
    - Interoperability Standards Priorities Task Force
        - Six meetings
        - Initial list of priority uses
    - Annual Report Workgroup
        - Three meetings
        - Kickoff and interactions with HITAC

Health IT Infrastructure Landscape Analysis

- Priority Target Area: Interoperability
    - Interoperability remains fragmented and uneven.
    - HHS has proposed regulations and a trusted exchange framework.

    - Work is underway to identify priority uses of health IT and associated standards and implementation specifications.
- Priority Target Area: Privacy and Security
    - Needed to advance and maintain trust in interoperability and protect patients.
- Priority Target Area: Patient Access to Information
    - Can have positive impact by supporting shared decision making.
    - More information, education, accessibility, and use of application programming interfaces (APIs) needed.

Health IT Infrastructure Gap Analysis

- The Cures Act requires an analysis identifying existing gaps and opportunities in policies and resources for achieving the ONC FY18 objectives and benchmarks and furthering interoperability throughout the health information technology infrastructure.

Recommendations for Addressing Gaps

- The Cures Act requires recommendations for HITAC activities to address the health information technology infrastructure gaps identified.

Priority Target Area: Interoperability

- Key Gap: Need to increase level of interoperability
    - Key Opportunity
        - Address “reality gap” between the perception of what has been certified for a system and what is truly interoperable in the field
    - Recommended HITAC Activity
        - Further measure whether systems are truly interoperable at both content and transport levels after implementation, especially among smaller practices and by patients

Priority Target Area: Privacy and Security

- Key Gap: Implications of emergence of the Internet of Things (IoT)
    - Key Opportunity: Consider appropriate policies for the IoT
    - Recommended HITAC Activity
        - Identify areas of IoT use that would benefit from guidance and examples of success in the health care industry 19 Priority Target Area: Privacy and Security
- Key Gap: Lack of user awareness and education about privacy and security protections
    - Key Opportunity: Offer support for and education of technology users regarding privacy and security protections, including for health and other information shared on social media
    - Recommended HITAC Activity
        - Identify educational approaches, technological mitigators, and potential regulatory solutions that offer improved privacy and security protections
- Key Gap: Variability of information sharing policies across states
    - Key Opportunity
        - Increased uniformity of information sharing policies across states
    - Recommended HITAC Activity

        - Consider federal role in setting guidelines for the exchange of data across states.
- Key Gap: Variability in adoption of cybersecurity framework(s)
    - Key Opportunity
        - Offer support for widespread adoption of cybersecurity framework(s).
    - Recommended HITAC Activity
        - Consider the impact of nationwide adoption of cybersecurity framework(s) and delineate cybersecurity accountability for data by role
- Key Gap: Lack of user control to share and disclose information
    - Key Opportunity
        - Consider options for granular levels of consent to share and disclose information
    - Recommended HITAC Activity
        - Undertake a review of emerging consent approaches and the technologies that underpin them, and make recommendations for the improvement of current consent approaches

Aaron Miri turned the review over to **Carolyn Petersen**.

Priority Target Area: Patient Access to Information

- Key Gap: Unmet infrastructure needs for underserved populations
    - Key Opportunity
        - Support infrastructure needs for underserved populations, including exchange costs, the prevalence of electronic equipment, Internet access, pharmacy services, and use of telehealth services
    - Recommended HITAC Activity
        - Measure impact of monetization of data exchange
- Key Gap: Accessibility and usability of patient portals and other patient-facing technology continue to need improvement
    - Key Opportunity
        - Consider improvements to accessibility and usability of patient portals and other patient-facing technology
    - Recommended HITAC Activity
        - Measure amount/length of time a portal has been online working properly, patient engagement, and/or patient understanding and use of data
- Key Gap: Patient awareness and education about health IT resources
    - Key Opportunity
        - Encourage patient and caregiver education about health IT resources
    - Recommended HITAC Activity
        - Identify use cases demonstrating the value of patient's data to the patient

Carolyn Petersen opened the discussion for questions and/or comments.

Discussion

Denise Webb questioned what consider meant in the recommendations.

- **Carolyn Petersen** shared that there is specific language that government typically uses and "consider" is something that is often used by government. That said, the HITAC has latitude and can consider what the committee thinks will be valuable going forward.

Denise Webb questioned what, "testing" is being referred to.

- **Carolyn Petersen** shared that it could be testing for heart rate monitors, as an example.
- **Denise Webb** asked that "clinical" be added for clarity.

Aaron Miri noted that Steven Lane shared comments on the annual report and urged additional HITAC members to share their feedback.

Carolyn Petersen also asked the members to share their feedback, asking for all comments to be shared by midnight on February 27, 2018. She also shared the importance of closing this work, understanding that members will be busy providing feedback on the NPRM.

Lauren Richie shared that members should send their feedback to onc-hitac@accelsolutionsllc.com.

Clem McDonald noted to be careful using the word unstructured in the document.

Ken Kawamoto asked whether the workgroup considered the current status of the patient name for the industry-standard protocol for authorization (OAuth 2.0), noting that it would be useful to ask if this was Health Insurance Portability and Accountability Act (HIPAA) compliant.

- **Aaron Miri** reminded the committee that the work was for the fiscal year 2018 and some of the items discussed hadn't yet come out during that time period.

Carolyn Petersen reminded the HITAC of the February 27, 2018 deadline and again thanked the members of the workgroup for their contributions.

There was additional time remaining; therefore, an opportunity was provided to members to ask questions about the NPRM. These items are included above in the discussion section of the NPRM.

Lauren Richie opened the lines for public comment.

Public Comment

Mari Savickis, CHIME: "I had a question which I know are hard to answer on an advisory committee. I want to find out if there is any information regarding educational webinars so we can get that information out to the members. Also, if there is an opportunity for people who are outside of the HITAC to participate in the task force? I wasn't clear about that. It sounds like they are getting started next week. This would be helpful. I also wanted to echo the comment that was made regarding the deadline. We have received feedback that more time will be needed. Thank you for taking my comment."

- **Elise Sweeney Anthony** responded that ONC tries to make sure there is as much engagement as possible. We will have a series of webinars for the general public around the NPRM. We are

working on finalizing the dates. They should be upcoming. Hopefully starting next week. We will publicize those online, so folks have it. In the interim I want to reiterate even though the rule is not included and has not been published in the federal register yet, it is currently online on the website at HealthIT.gov /NPRM. If there are any changes, they will be small changes and it will not be substantive changes. What you have on the website is what ONC is going out with in terms of the proposal. The website has several infographics and fact sheets. They lay out different sections of the rule. I think Steve noted earlier the goal is to provide a quick, relatively easy to read resource for you to take a quick look at the sections of the rule that can allow you to dig deep later. We will publish the webinar dates and times on the website. I would encourage folks to sign up quickly. Those tend to fill up quickly.

- **Lauren Richie** noted that on HealthIT.gov/HITAC there is a place for membership applications to apply for task forces. There is a drop-down menu that includes all the task forces. If an application has already been submitted, there is no need to submit it again.

Comments in the public chat during the meeting

Patricia Falto, MSc: Question - If a part of a patient's record is missing due to the patient having a duplicate MRN, can information blocking penalties be applied due to this error? Just checking.

Timothy Bennett: What would be the timeline for implementing the NCPDP 2017017 version of the ERX standard as part of b.11? that wouldn't be a 2-year implementation timeline given CMS 2020 deadline for this standard use, right?

Michael Lipinski: There is no proposed certification deadline for NCPDP 2017017. Our proposed approach is to permit certification to both standards (10.6) until such time 10.6 is no longer permitted for Part D, which is currently specified as 1/1/2020.

Michael Lipinski: this assumes we issue a final rule with an effective date prior to the Part D date.

Gay Dolin: @Steve:

Gay Dolin: I find a Lack of Clarity with definition of what/who an API User is

Gay Dolin: Sorry if I missed something -- had to drop for a bit:

Gay Dolin: I suggest dividing these roles into two roles and clarifying the fee rules for once each role is defined. API Patient/Person/Consumer User: Persons that use software applications that interact with API Technology. API Technology Supporter: Entity/HIT Developer that creates software or content applications that interact with or enable the API Technology supplier software

Steve (onc): These roles are divided/described in the rule's preamble in more detail

Gay Dolin: I know :-)

Gay Dolin: Read them

Steve (onc): The proposals do not treat the division of roles you've noted different when it comes to fees, but it's certainly something on which you and others can comment (thanks in advance)

Gay Dolin: Can an API User charge an API Data provider or an API technology Provider - or rather are there discussion with respect to that direction of permitted fees in the NPRM that I missed?

Ken Kawamoto: @Steve - is the TF that covers what you discussed be the Conditions of Certification one?

Steve (onc): Ken, yea, the Conditions of Certification TF would have the API CoC in its scope. the other Info Blocking TF would have some of the IB related CoCs

Ken Kawamoto: thanks

Denise Webb: Is ONC permitting others besides HITAC members to participate on the task forces (via application on Website)?

Carl Johnson: I'm new to the process. How does one get involved with a task force?

Aaron Miri: Volunteer! The TF's are always looking for folks to volunteer. https://www.healthit.gov/topic/federal-advisory-committees/membership-application

Carl Johnson: thank you Aaron! Will do1

Steve (onc): @Gay, we do cover a little bit about the directionality of the permitted fees (e.g., who they can be between, how they can be paid and by whom). When it comes "API User" insofar as it would be a 3rd party app/service and its market behavior is not explicitly covered by the Cures Act.

Clement J McDonald: We have to be careful about the use of "unstructured" because there must be some structure, e.g. patient ID, date think they really mean payload is narrative but not that the content is unstructured

Clement J McDonald: The USCDI in the report does not mention Imaging reports, thought they are prominently presented in the NPRM. Seems like they should be in the UCSDI

Clement J McDonald: Argonaut vs FHIR profiles is apt.

Sasha TerMaat: Steve, if a supplier decides not to verify application developers, or to do so automatically, is there clarity that they are not liable for consequences that might occur because of the lack of vetting?

Gay Dolin: @Steve - Thanks for your earlier answer -- that really helps

Next Steps and Adjourn

The next meeting is scheduled for a two-day in-person meeting on March 19 - 20, 2019.

Lauren Richie reminded the HITAC to respond to the email that was shared regarding travel. She also noted that she will follow-up with the details Michael Lipinski reviewed regarding the task forces that will review the NPRM.

Carolyn Petersen thanked everyone again.

Robert Wah noted that he was looking forward to seeing everyone in person in March.

The meeting was adjourned at 1:00 p.m. ET