Table of Contents

• Introduction—Why Apps?

• What ONC is doing to advance use of Apps and APIs in health care
  » Certified EHR Technology (CEHRT)
  » How CEHRT Automates Permitted Uses and Patient Access

• What about privacy & security?
  » HIPAA and Health Information Exchange
  » HIPAA Permitted Uses
  » HIPAA Patient Access
  » ONC API Task Force: Addressing Privacy & Security Concerns about APIs

• OCPO Resources and Tools

• Questions?
Why Healthcare APIs?

• Brings data into the reach of everyone
• Can break data up into chunks which become easier to use and analyze
• Increases interoperability for better healthcare outcomes
• Automates movement of data
• Lowers cost of integration
APIs- Common Clinical Uses

APIs are used today to:

• Connect functionalities among peer systems within a larger organization,
  » Within healthcare to share common clinical data within an organization or system.
• Combine functionalities among two or more vendors' systems to provide a desired set of functions,
  » to request clinical tests and obtain results for incorporation into a patient’s clinical record.
• Connect functionalities with external organizations, e.g., standalone laboratories, standalone imaging centers, providers, researchers, payers etc.
Why Apps? Why Open APIs?

- Apps meet the patients and caregivers where they are.
- Patients and Caregivers want:
  - Online access to view, download and transmit copies of their health information
  - Access patient-specific educational information
  - Send and receive secure messages to their providers
  - Request appointments and medication refills
- Open APIs (APIs that third party apps can access) answer the need of a diverse patient universe; individuals are not “one size fits all”.
  - Varying languages
  - Varying support & caregiving environments
  - Varying health situations
  - Varying
How APIs and CEHRT Fit Into the Picture

• APIs can enable health information to be shared between systems and via third-party apps

• Can support exchange of information as allowed or required by HIPAA
  » For example, enable one provider’s system to request and obtain clinical test results from another provider’s system. More info available at healthit.gov.

• Can support patient electronic access to health information for purpose of HIPAA Access Rule
  » For example, enable patient to use a third-party app to access their PHI from provider’s system. More info from OCR, more info from ONC.
Apps and APIs Build On HIPAA’s Support for Interoperability

• HIPAA Privacy Rule Permits, and sometimes Requires Information Exchange

• HIPAA permits exchange between covered entities for
  – Treatment, Payment, and Health Care Operations
  – More detail on ONC/OCR Fact Sheets and blogs on HealthITbuzz

• HIPAA requires disclosure of PHI when requested by an individual
  » Gives patients the right to access their health information electronically if stored electronically
  » Provides patients with the right to send a copy of their information to a third party
  » That copy can be required to be in an electronic format if the disclosing provider has that capability.
    – “Further, as technology evolves and PHI becomes more readily available via easy-to-use digital technologies, the ability to provide very prompt or almost instantaneous access to individuals will increase. The Department [OCR] will continue to monitor these developments.”
HIPAA Permitted Uses Drill Down

- **MYTH:** HIPAA makes it impossible to exchange health information electronically for patient care

- **FACT:** HIPAA permitted uses actually *allow* health information to be exchanged in a number of specific circumstances
  - Providers can share PHI for **treatment**, broadly defined to include things like referrals, care management by someone hired by the provider, or transitions of care
  - Providers and payers can share PHI for **operations** such as quality improvement, care coordination and other activities
  - Under HIPAA, this type of sharing does not require a written patient authorization; however, other laws or organizational policies may impose such requirements.
  - Information can be shared electronically, supporting interoperability and making **information available to the right people at the right time for patient care**

- **ONC** is releasing **fact sheets** and a series of **blog posts** with numerous examples of when electronic health information can be exchanged
Permitted Uses Drill Down: Key Concepts for Exchange between Covered Entities

• “May” = discretion
  » Lawyers call it “permitted uses or disclosures”
  » Permitted is a key concept: it is the Covered Entity’s choice
  » BAs can undertake the disclosure function on CEs behalf
    – E.g. HIEs

• Minimum necessary applies

• What is permitted:
  » Access, use and disclosure for a covered entity’s own treatment, payment or health care operations
  » Access and use by another CE, or disclosure to the other CE, for the recipient CE’s treatment, payment or health care operations
Patients have a **right** to see, receive a copy, or request that a copy of their medical records be sent to a third party the patient chooses. *(45 CFR § 164.524)*

- If records are stored electronically, patients have a right to an **electronic copy of their records**
- ONCs 2014 Edition Rule, requiring the ability for an individual to view/download/transmit PHI, helps automate HIPAA right to
- Read ONC’s access blog post [here](#)

### Actions taken by patients accessing electronic medical records

<table>
<thead>
<tr>
<th>Action</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sent the information somewhere else, such as to a PHR</td>
<td>11%</td>
</tr>
<tr>
<td>Downloaded the information to computer or mobile device</td>
<td>39%</td>
</tr>
<tr>
<td>Shared the information with someone else</td>
<td>44%</td>
</tr>
</tbody>
</table>

*Source: ONC’s 2013 Consumer Survey of Attitudes Toward the Privacy and Security Aspects of Electronic Health Records and Health Information Exchange*
HIPAA Patient Access Drill Down:

- HHS Office for Civil Rights enforces this individual right
  - Follow OCR on Twitter: @hhsocr
  - [http://www.hhs.gov/hipaa](http://www.hhs.gov/hipaa)

- OCR issued **new guidance** on January 7. Key concepts for apps and APIs
  - Timing
  - Automation
  - Electronic formats

- This right has some limits:
  - Provider can reject media (such as a thumb drive) that reasonably threaten the security of the provider systems
  - Psychiatric notes and prison medical records can be withheld.
  - There are other limits that the individual can appeal.
How 2015 CEHRT Automates Permitted Uses and Patient Access

Under HIPAA
- Health information can be shared for permitted uses (TPO)
- Patients have the right to an electronic copy of their medical records, if the records are stored electronically, and right to send a copy (transmit) elsewhere

MU Stage 3 Requirements
Patient must be given electronic access to portal within 24 hours in order to
- view online, download and transmit their health information
- AND access to an API that can be used by 3rd party apps

Related CEHRT Requirements
- API functionality including
  - lookup and retrieve whole or partial patient record
- API security measures
- A “transmit” option that includes unencrypted email
• Three API criteria
  » Lookup a patient
  » Retrieve part of a patient record
  » Retrieve an entire patient record

• Required security criteria
  » Authentication, authorization, & access control
  » Auditing
  » Encryption
“Transmit” in the 2015 Edition Certification Rule

• VDT = View, Download, Transmit

• In 2015, new method to satisfy “transmit” criteria (must have capabilities for both):
  
  » Unencrypted option – Used at patient direction to email to a patient-specified email address
    
    – Cannot be used for provider-to-provider exchange; only for patient-directed movement
  
  » Encrypted option – an encrypted method identified by the HIT developer (e.g., Direct, encrypted email, etc.)
ONC API Task Force: Addressing Privacy & Security Concerns about Open APIs

• Identify perceived security concerns and real security risks that are barriers to the widespread adoption of open APIs in healthcare
  » For risks identified as real, identify those that are not already planned to be addressed in the Interoperability Roadmap (for example, identity proofing and authentication are not unique to APIs)

• Identify perceived privacy concerns and real privacy risks that are barriers to the widespread adoption of open APIs in healthcare
  » For risks identified as real, identify those that are not already planned to be addressed in the Interoperability Roadmap (for example, harmonizing state law and misunderstanding of HIPAA)

• Identify priority recommendations for ONC that will help enable consumers to leverage API technology to access patient data, while ensuring the appropriate level of privacy and security protection
API TF testimony - Important Facts Shared on APIs

• API Resources can regulate how, when, and who uses the API

• APIs provide a well-documented, popular way for organizations to share access to data and services with third parties, while maintaining strict security controls.

  » Clear and Concise documentation is important for open standard APIs

• API is extremely precise and allows the opportunity for all the right levels of access and security, e.g. data granularity

• Technical solutions exist for technical problems

• Need consensus best practices to help secure the API

• Business & legal considerations may remain.

  » Does it matter if the discloser “owns” the PHI or not?

  » Provider liability and accountability for data usage and breach, even though OCR/ONC Fact sheets say a discloser is not liable for what a receiver does with data so long as the discloser discloses the data properly.
API TF testimony – Consumer Perspective

• More Access, More Patient Control, More Engagement
  ✓ A panelist indicated access to his data helped save his own life, and asked “why can’t patients have access to more of their own data?”

• Choices should be given to patient, and patients are smart enough to make privacy & security choices that are right for them.

• Systems should account for diverse consumers:
  » some want personally to control every decision;
  » some want health information to move where it needs to go without them having to manage that process.

• Transparent data practices are important for consumers

• Role of HIPAA in protecting consumer vs. protections outside HIPAA

• Recordings/transcripts available here:
  » Jan 26:  https://www.healthit.gov/facas/calendar/2016/01/26/api-task-force-virtual-hearing
  » Jan 28:  https://www.healthit.gov/facas/calendar/2016/01/28/api-task-force-virtual-hearing
• Support for Open Standards-based APIs.

• Who do you trust? How do you know that person is accessing your system?
  » Need to verify identity of person accessing system, even through an app.
  » Need to verify that the app is operating on behalf of a verified person.
  » Who is accessing and which apps are in use varies by role:
    – Patient/individual/caregiver
    – Provider
    – Information systems administrator

• Long term, protections will be in place to allow for varying levels of access.

• Business and legal issues.
OCPO Resources and Tools

- Permitted Uses Fact Sheets
- OCR Patient Access Guidance
- Privacy and Security Guide
- Mobile Device Web Pages
- Cybersecurity Web Pages
- Cybersecurity Game – Medical Planning/Contingency Planning
- Model Notices of Privacy Practices
- Risk Assessment Tool
- Data Segmentation Resources
Upcoming OCPO Resources

• API Taskforce Recommendations
• FTC Navigator Tool
• Consumer materials on right of access
(7) Application access—patient selection. The following technical outcome and conditions must be met through the demonstration of an application programming interface (API).

(i) Functional requirement. The technology must be able to receive a request with sufficient information to uniquely identify a patient and return an ID or other token that can be used by an application to subsequently execute requests for that patient's data.

(8) Application access—data category request. The following technical outcome and conditions must be met through the demonstration of an application programming interface.

(i) Functional requirements. (A) Respond to requests for patient data (based on an ID or other token) for each of the individual data categories specified in the Common Clinical Data Set and return the full set of data for that data category (according to the specified standards, where applicable) in a computable format.

(9) Application access—all data request. The following technical outcome and conditions must be met through the demonstration of an application programming interface.

(i) Functional requirements. (A) Respond to requests for patient data (based on an ID or other token) for all of the data categories specified in the Common Clinical Data Set at one time and return such data (according to the specified standards, where applicable) in a summary record formatted according to the standard specified in §170.205(a)(4) following the CCD document template.

(C) Transmit to third party. Patients (and their authorized representatives) must be able to:

(1) Transmit the ambulatory summary or inpatient summary (as applicable to the health IT setting for which certification is requested) created in paragraph (e)(1)(i)(B)(2) of this section in accordance with both of the following ways:

- (i) Email transmission to any email address; and
- (ii) An encrypted method of electronic transmission
• “What’s an API” presentation to the ONC Joint API Task Force:
  » https://www.healthit.gov/facas/calendar/2015/12/04/joint-api-task-force
Permitted Uses and Treatment Fact Sheets

- **ONC Fact Sheets** focusing on treatment and health care operation activities that do not require patient consent

- Many of these permitted uses and disclosures support interoperability, including:
  - Care coordination & Case Management
  - Care planning
  - Quality Assessment/Improvement
  - Population-Based Activities
OCR Patient Access Guidance and Related Blog Posts

• OCR Patient Access Guidance

• OCR Patient Access Blog Post
  – http://www.hhs.gov/blog/2016/01/07/understanding-individuals-right-under-hipaa-access-their.html#

• ONC Patient Access Blog Post
April 2015 Updated Guide focuses on:

- Privacy and security requirements for EHR Certification Criteria - 2014 Edition
- Updated privacy and security requirements resulting from HIPAA modifications
- New, practical examples of the HIPAA Privacy and Security Rules in action

Developed in coordination with HHS Office for Civil Rights and Office of General Counsel

Mobile Device Materials Available Online

- Materials available on [HealthIT.gov/mobiledevices](http://HealthIT.gov/mobiledevices) include:
  - Fact sheets
  - Posters
  - Brochures
  - Postcard
  - Educational videos
Cybersecurity Web Pages

- Cybersecurity Resources for the Health Care Sector
- Link to National Institute of Standards and Technology (NIST) Cybersecurity Framework

http://www.healthit.gov/providers-professionals/cybersecurity-shared-responsibility
Cybersecure: Medical Practice

A training game that requires users to respond to privacy and security challenges often faced in a typical small medical practice.

http://www.healthit.gov/providers-professionals/privacy-security-training-games
The latest training game focuses on disaster planning, data backup and recovery and other elements of contingency planning.

http://www.healthit.gov/providers-professionals/privacy-security-training-games
The Office for Civil Rights (OCR) and Office of the National Coordinator for Health Information Technology (ONC) collaborated to develop model NPPs for covered entities to use:

- One set for health plans
- One set for health care providers
HHS Security Risk Assessment (SRA) Tool

• Downloadable SRA Tool designed to guide providers through the Risk Assessment process.

• Tool includes resources to:
  – explain the context of the question,
  – provide examples of potential impacts to PHI, if requirements are not met
  – identify examples of safeguards to help mitigate identified risks and vulnerabilities

Data Segmentation Resources and Website

• ONC successfully completed a three year project (the Data Segmentation for Privacy initiative) which developed and piloted standards to help integrate behavioral health-related information into the primary care setting.

• The HIT Policy Committee approved recommendations that the DS4P document-level standards be included as voluntary Certified EHR Technology (CEHRT) for Meaningful Use Program Stage 3.

• The information (including the balloted standards) is available on the healthit.gov website.

http://www.healthit.gov/providers-professionals/data-segmentation-and-you