The Office of the National Coordinator for Health Information Technology

Office of the Chief Privacy Officer

National Committee for Vital & Health Statistics
June 15, 2016
Lucia Savage, J.D.
ONC Chief Privacy Officer

ONC OCPO Update

- Consumer Education on Right of Access
- HIPAA Basics
- API Task Force Draft Recommendations
- Cybersecurity

HIPAA Right of Access

- HIPAA requires disclosure of PHI when requested by an individual
  - Gives patients the right to access their heath 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."
  - The third party can be an app, a competing provider, a friend or a family member
  - It is ok for the person to request unencrypted email as the transmit method

To Educate Consumers, We Made Some . . .

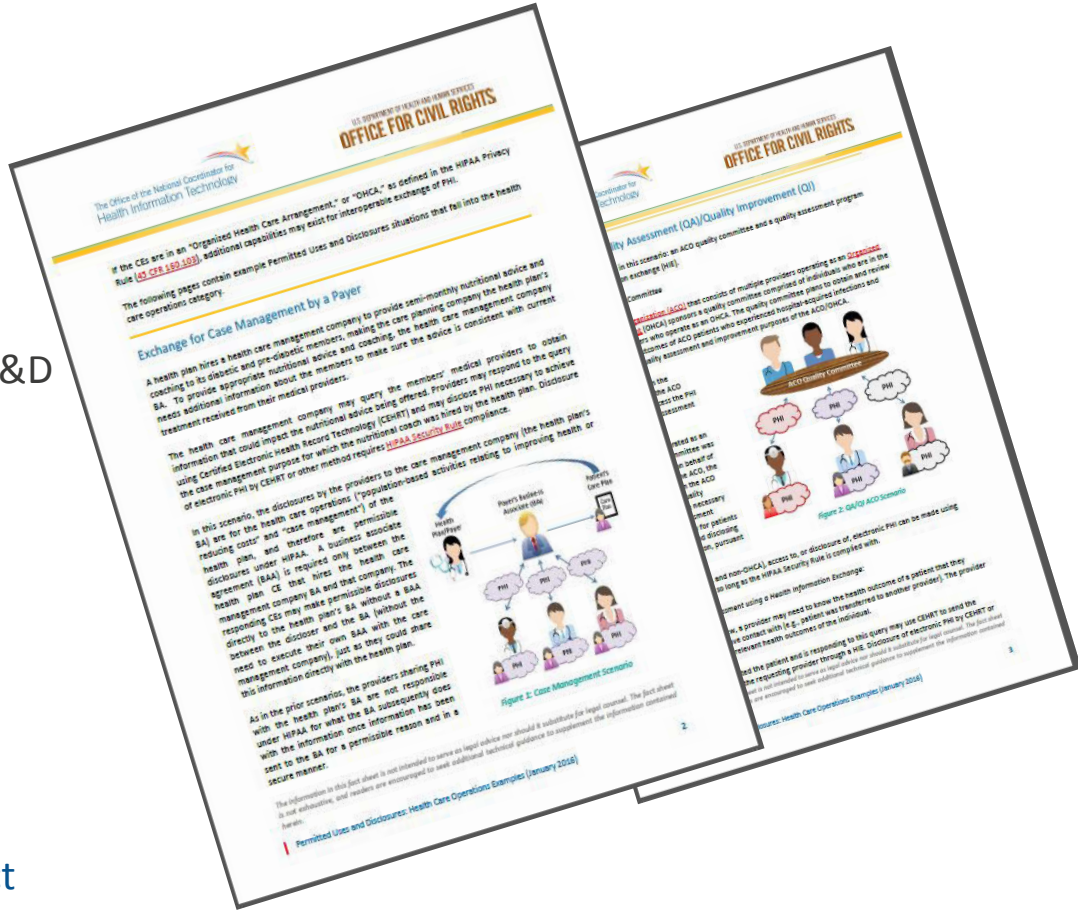
- Movies
  - » https://www.healthit.gov/access
- Infographic
  - » https://www.healthit.gov/access
- More materials coming
- Captioned in Spanish and English

Other Patient Access Resources

- OCR Patient Access Guidance
  - http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html
- 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
  - http://www.healthit.gov/buzz-blog/privacy-and-security-of-ehrs/your-rights-to-access-and-transmit-your-health-information/

HIPAA Basics: The Real HIPAA Supports Interoperability--OCPO Blog Series

- OCPO launched a 4-part blog series entitled the "Real HIPAA Supports Interoperability" on February 4
  - » Blog 1: The Real HIPAA Supports Interoperability
  - » Blog 2: Background on HIPAA's PU&D
  - » Blog 3: Examples of Care Coordination, Care Planning, Case Management
  - » Blog 4: Examples of Quality Assurance and Population-Based Activities
- OCPO/OCR co-branded educational fact sheets that provide practical, plain language, examples with illustrations to supplement the blog series.

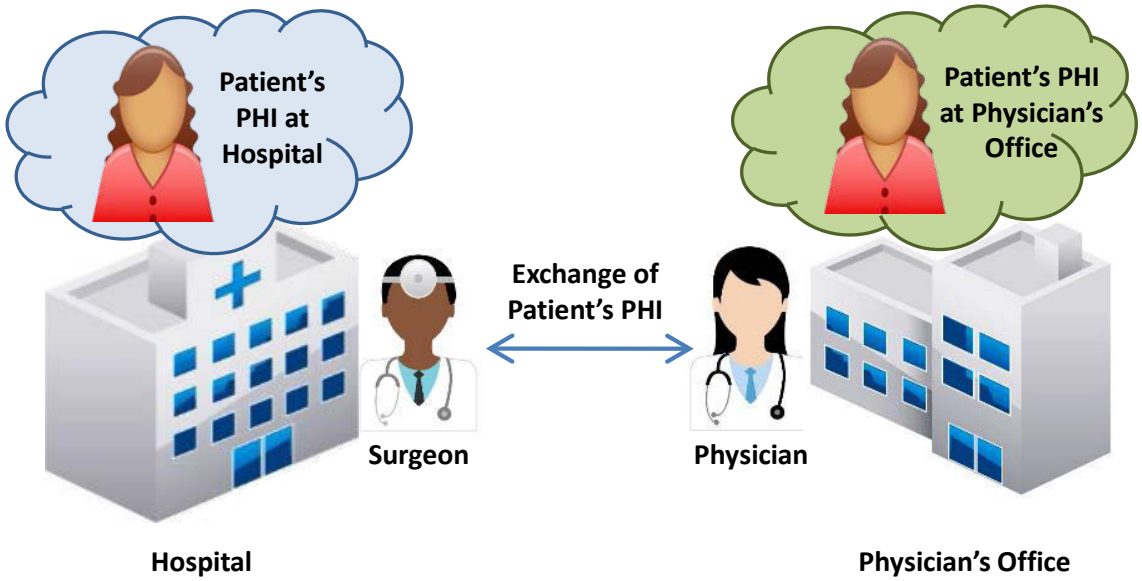


https://www.healthit.gov/newsroom/fact-sheets
Permitted Uses and Disclosures: Exchange for Health Care Operation [PDF - 1.3 MB] *
Permitted Uses and Disclosures: Exchange for Treatment [PDF - 1.1 MB] *

What are Permitted Uses and Disclosures--*Treatment*

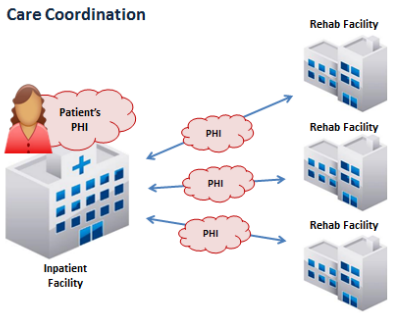
- Permitted Uses and Disclosures (PU&D) are situations in which a covered entity is permitted, but not required, to use and disclose PHI without first having to obtain a written authorization from the patient.

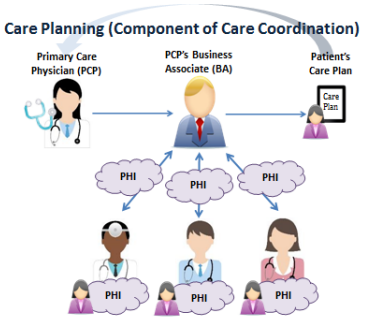
Basic Illustration of Permitted Uses

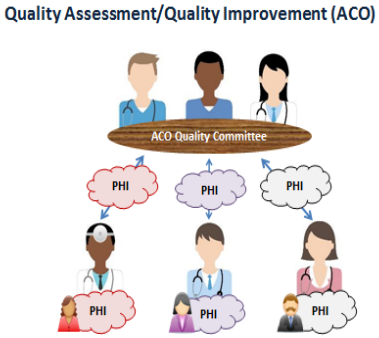


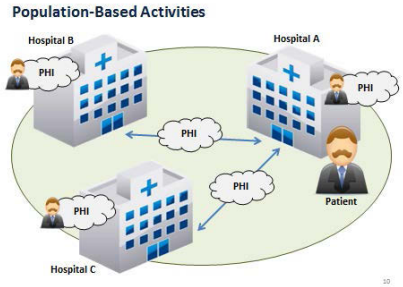
Permitted Uses Fact Sheets

- Conducting quality assessment and improvement activities
- Conducting case management and care coordination (including care planning)
- Conducting population-based activities relating to improving health or reducing health care cost
- Developing protocols
- Evaluating performance of health care providers and/or health plans









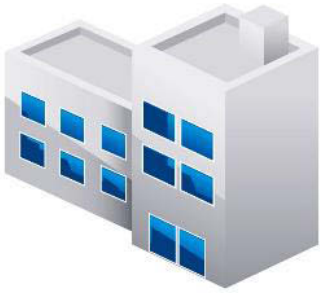
https://www.healthit.gov/newsroom/fact-sheets
Permitted Uses and Disclosures: Exchange for Health Care Operation [PDF - 1.3 MB] *
Permitted Uses and Disclosures: Exchange for Treatment [PDF - 1.1 MB] *

HIPAA Permitted Uses Allow Exchange of MH and BH Information

Patient's with Behavioral Health PHI

Exchange of Patient's MH PHI

Primary Care Provider



Physician's Office

Exchange of Patient's MH PHI

Licensed Professional Counselor

Exchange of Patient's MH PHI

Behavioral Health Clinic

Basic Choice: When is Opting required by law and what are the implications of such a requirement?

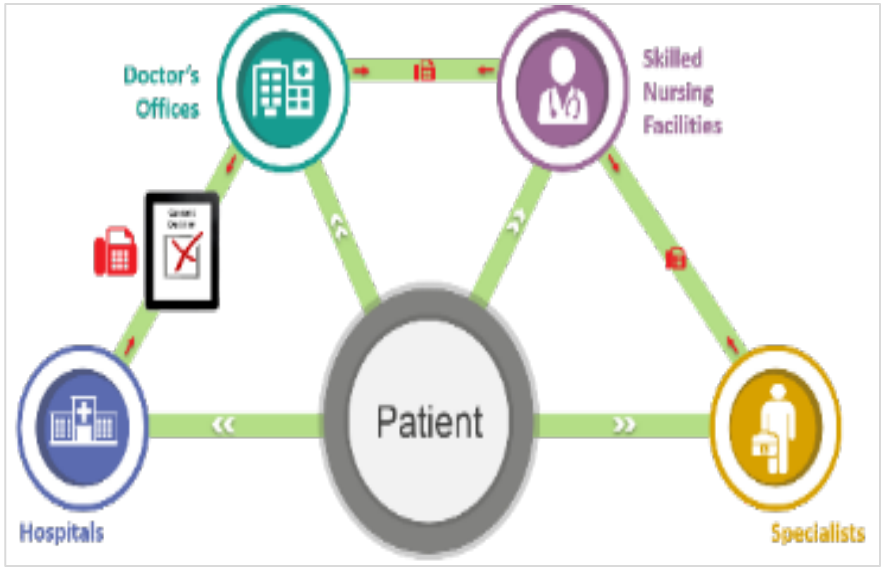
- **Our Final Interoperability Roadmap states:**

  By the end of CY 2016 ONC will identify a definition of "Basic Choice" and provide policy guidance regarding if/when Basic Choice should be offered, even when not required by law, based on recommendations from the HITPC by the end of CY 2016.

- **ONC can**

  - » Clarify the interoperability and health implications of offering choices about electronic exchange that are not offered about other media

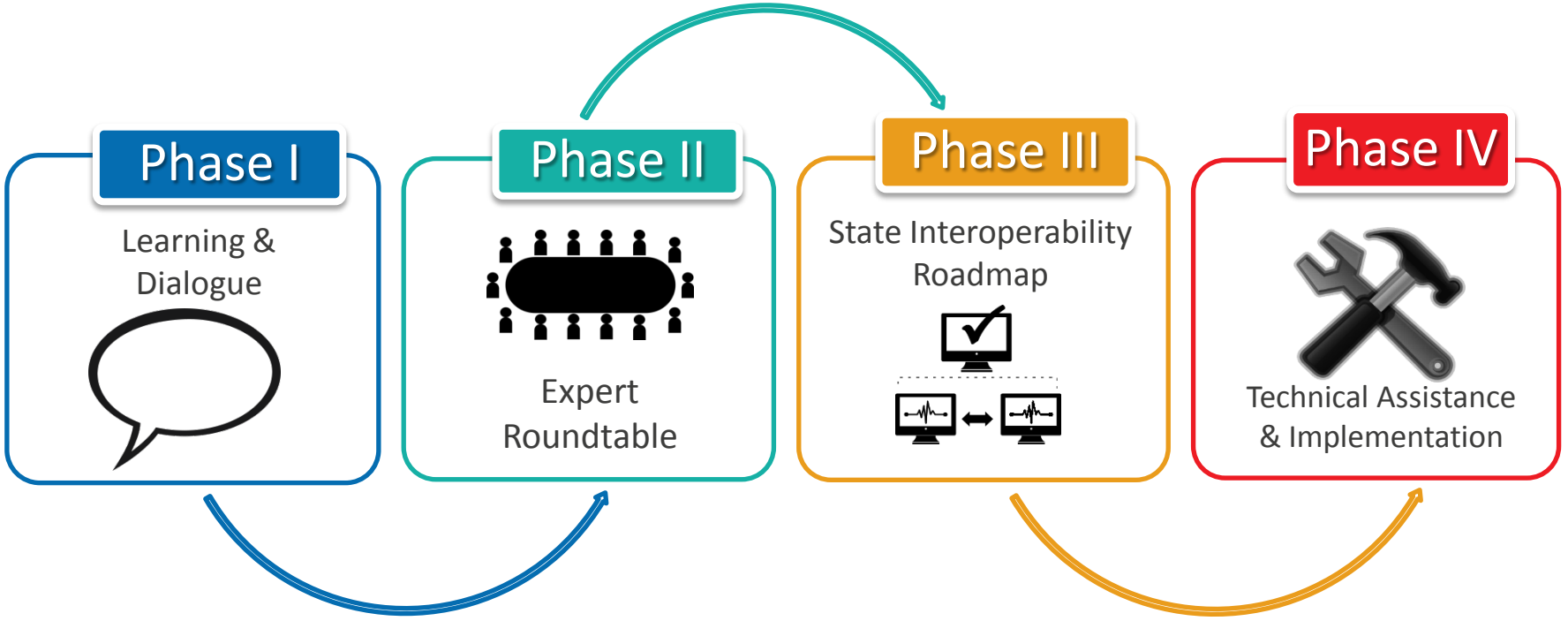
- **ONC will refer to Basic Choice as a policy decision to offer opt-in or opt-out of electronic exchange as a general concept.**



Part of a larger campaign to make privacy compliance automated and computable: [new computable privacy web pages]

NGA Project – Developing a State Interoperability Roadmap

Timeline and Objectives Sept 2015 to May 2017



The Office of the National Coordinator for Health Information Technology

API Joint Task Force charge:

- **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.**

Out of Scope for API TF

- **MOTIVATION FOR LIMITED SCOPE**
- Ultimately, the Task Force focused on needs specific to MU3 requirements and 2015 CHIT. Specifically, our recommendations focus on *read-only access to a single patient's record for disclosure to an app selected by that patient, and used to access all or some data elements defined in the Common Clinical Data Set*.
- Other "out of scope" issues include:
  - Terms of Use
  - Licensing Requirements
  - Policy Formation
  - Fee Structures
  - Certifying Authorities
  - Formulation of Standards
  - Electronic documentation of consents required by law or policy
  - Issues unique to writing new data into the EHR
  - Issues unique to annotating data in the HER
  - Health efficacy of the apps themselves

APIs in the 2015 Edition Certification Rule

- 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

Timeline

- Task Force Meetings November 2015 through May 2016
- Final recommendations submitted to Joint Federal Advisory Committee May 17, 2016
- Audio file available at: https://www.healthit.gov/facas/calendar/2016/05/17/joint-hit-committee-meeting

Some of the API TF Recommendations

- It is ok to require apps to register themselves, but that should not cause undue burdens to patients pursuing their right of access
- Voluntary, private sector led app accreditation programs should be encouraged *and* physicians should continue to counsel and collaborate with their patients about using apps
- While providers releasing data to an app via an API must continue to protect the security of their own system, it was also recognized that how a patients-chosen app uses data downstream is not within scope for the protection of the provider's system
- ONC should continue to collaborate with FTC, OCR and other agencies to improve patients health and privacy literacy
- ONC should expand CERHT criteria to ensure that an API's audit trail is available to an individual under the HIPAA Accounting for Disclosure rule.
- ONC clarify the applicability of identity proofing and authentication standards for use of patient-chosen apps requesting data from an API

Security –detailed agenda

- Security Topics
  - Identity proofing
  - Cyber Information Sharing Act of 2015
  - Ethical Hacking

Identity Proofing

- D3. Commitments 1. ONC, in consultation with stakeholders, will establish and adopt best practices for provider and individual/consumer identity proofing and authentication, including specific levels of assurance, and will consult with OCR to ensure they are consistent with the HIPAA Security Rule and best practices already adopted for other comparable industries.

Announcing Draft Special Publication 800-63-3: Digital Authentication Guideline!

Posted on May 8, 2016 by Paul Grassi

Today, we're releasing the public preview of draft Special Publication 800-63-3, Digital Authentication Guideline. We're excited to share the updates we've made—along with the new process that enables our stakeholders to contribute to the document in a more dynamic way.

Cyber Information Sharing Act of 2016

Internal Analysis and Reporting	(b)(1)) Report.— (1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Secretary shall submit to the Committee on Health, Education, Labor, and Pensions of the Senate and the Committee on Energy and Commerce of the House of Representatives a report on the preparedness of the Department of Health and Human Services and health care industry stakeholders in responding to cybersecurity threats.
Threat Sharing Task Force	(c) Health Care Industry Cybersecurity Task Force.—(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Secretary, in consultation with the Director of the National Institute of Standards and Technology and the Secretary of Homeland Security, shall convene health care industry stakeholders, cybersecurity experts, and any Federal agencies or entities the Secretary determines appropriate to establish a task force to—
Security Standards Task Force	(d) Aligning Health Care Industry Security Approaches.—(1) IN GENERAL.—The Secretary shall establish, through a collaborative process with the Secretary of Homeland Security, health care industry stakeholders, the Director of the National Institute of Standards and Technology, and any Federal entity or non-Federal entity the Secretary determines appropriate, a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes that

Ethical Hacking

- According to Politico Cybersecurity May 12, 2016:
  - Defense Secretary Ash Carter said he was impressed by the "Hack the Pentagon" program, the first phase of which ends today. More than 1,400 hackers signed up for the bug bounty pilot initiative targeting Pentagon websites, with more than 80 bugs discovered that qualified for payouts so far. "All of this is helping us be more secure, at a fraction of the cost that exhaustively diagnosing ourselves would take," he said. "And we believe this approach, effectively crowd-sourcing cybersecurity, has great potential for us, as it does for a number of you around the table." ‘
- If ethically hacking the Pentagon is helpful, how could this help security in the healthcare sector?