The Office of the National Coordinator for Health Information Technology

ONC Update

Safeguarding Health Information: Building Assurance through HIPAA Security

8th Annual HIPAA Security Conference

September 2, 2015

Putting the I in HealthIT

www.HealthIT.gov

Outline

1. Supporting improved Cyber and Security response:
   - Assessing Risks from "New" Technologies
   - Importance of Information Sharing
   - Security Best Practices Healthcare Can Adopt from Other Industries
     - ONC Free Resources
2. Identifying Health IT Standards to improve security and expand interoperability
   - Identity Proofing and Authentication
   - Bringing NIST Framework to life for small healthcare businesses

Assessing Risks from "New" Technologies

- New to healthcare, but not new technology
  - Mobile, cloud, APIs
- Reuse lessons learned & best practices from other industries
- Threat sharing—Threats not unique to health care

Why Does Cyber Threat Information Sharing Matter?

- In an ***interoperable, interconnected health system***, an intrusion in one system could allow intrusions in multiple other systems.
- ***volume, timeliness, and quality***
- ***Better information yields better prevention***.

Information Sharing: Drivers and Mechanisms

Putting the I in Health IT
www.HealthIT.gov

Recent Healthcare Data Breaches

Executive Orders and Administration Priority

Draft Nationwide Interoperability Roadmap

Draft Federal Health IT Strategic Plan

Executive Order 13636 (2013) Overview

Putting the I in HealthIT
www.HealthIT.gov

EO 13636 directs the Executive Branch to:

- Develop a technology-neutral voluntary cybersecurity framework
- Promote and incentivize adoption of cybersecurity practices
- Increase volume, timeliness, and quality of **cyber threat information sharing**
- Incorporate strong privacy and civil liberties protections into every initiative
- Explore use of existing regulation to promote cyber security

Source: http://www.dhs.gov/sites/default/files/publications/EOPPD%20Fact%20Sheet%2012March13.pdf

Executive Order 13691 (2015) Overview

Putting the I in HealthIT
www.HealthIT.gov

EO 13691 Highlights

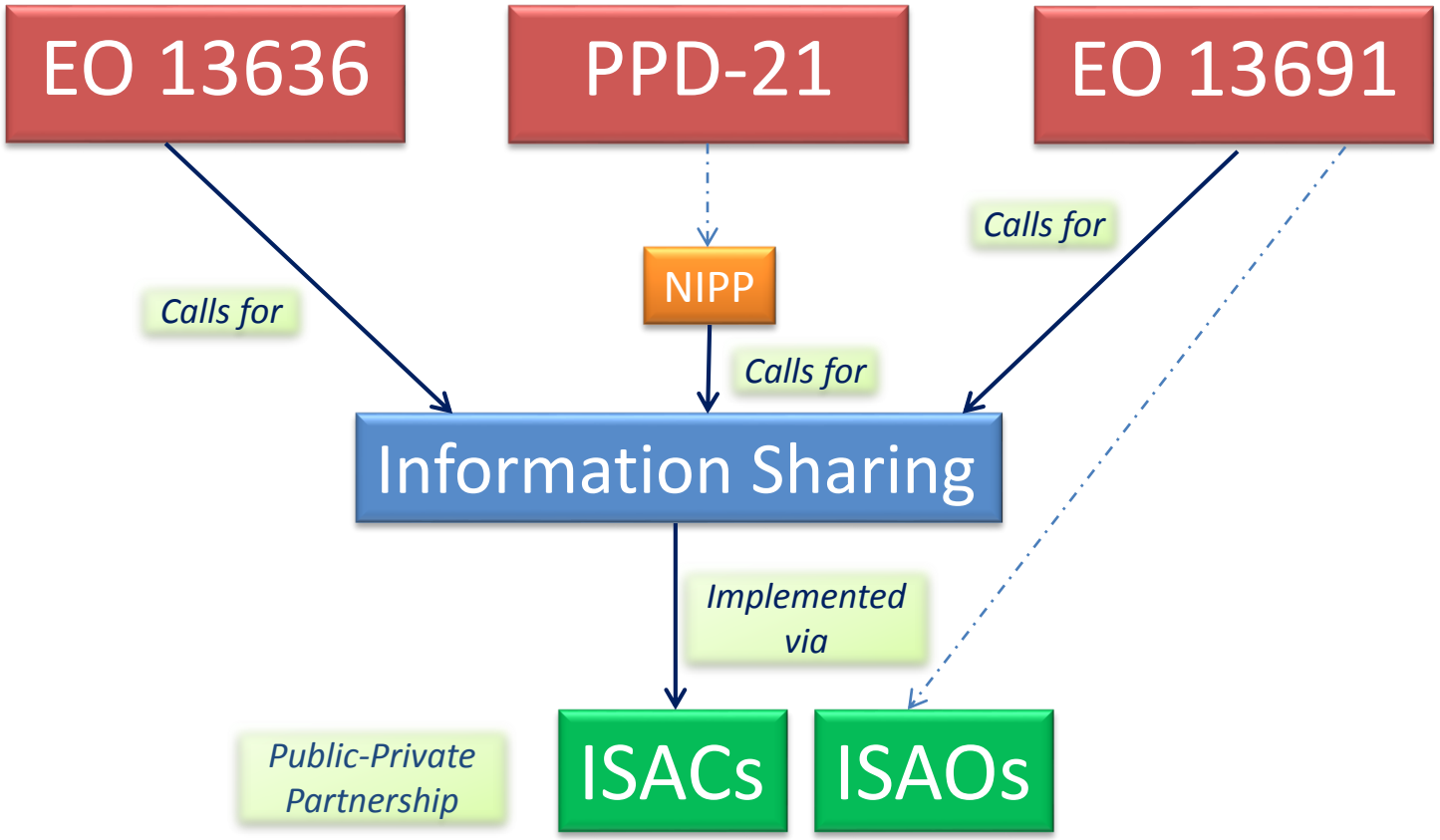
- Strongly encourages the development and formation of **Information Sharing and Analysis Organizations (ISAOs)**
- Provide strong Privacy and Civil Liberties Protections
- Create a Standards Organization (SO) and develop a common set of voluntary standards or guidelines for ISAOs
- Designates the NCCIC as a CIPP and delegates to authority to enter into voluntary agreements with ISAOs
- Streamline private-sector companies' access to classified cybersecurity threat information

Source: http://www.whitehouse.gov/the-press-office/2015/02/12/fact-sheet-executive-order-promoting-private-sector-cybersecurity-inform

NCCIC – National Cybersecurity Communications Integration Center

Policy Relationship Diagram

To protect critical infrastructure, the Executive Branch is directed to increase cyber threat information sharing and assigns HHS as the Sector-Specific Agency for the HPH Sector to enhance security and resilience with respect to all hazards, including cyber threats



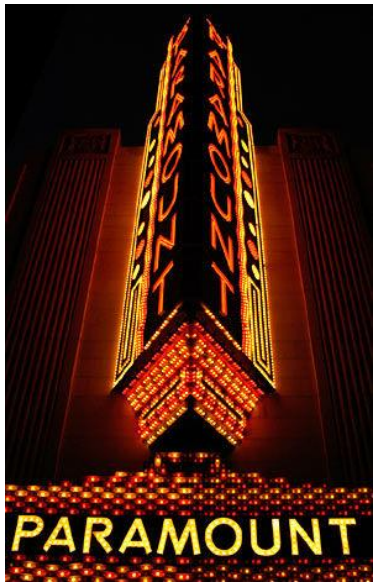
Security Best Practices We Can Adopt from Other Industries

- Data isolation
  - E.g., Store demographic identifiers in a separate encrypted database
- Fraud detection
  - E.g., operational monitoring
- Building Security In
  - E.g., penetration testing
- Asses Risk and remediate it

ONC Free Resources

- Security Risk Assessment Tool
  http://www.healthit.gov/providers-professionals/security-risk-assessment-tool
- Guide to Privacy and Security of Electronic Health Information
  http://www.healthit.gov/providers-professionals/guide-privacy-and-security-electronic-health-information
  - See Chapter 6: pull out guide to health IT Security
- OCR's website
  http://www.hhs.gov/ocr/

Coming soon . . .



- Best Privacy & Security Practices for mobile health developers—with OCR, FTC and others
- Privacy & Security Framework for PCOR
- Security Principles for Precision Medicine, supporting NIH

Identity Management

- We want to be confident that those who access systems are who they say they are, and should be accessing the system:
  - Need solutions users will use.
  - Build on best practices from other industries
  - Right-size the solution for the problem:
    - Individual access to their own PHI
    - Physician's office practice to patient panel data
    - IT System Administrator access to data from many practices.
- Avoid redundancy = rely on identity proofing others have confirmed.
  - Build on best practices from other industries
- Account for pervasive consumer use of smart phones.
  - Meet Consumers where they are.
  - Diverse Populations
- ONC is developing guidelines on patient and provider identity proofing and authentication using NIST Level of Assurance guidelines

Interoperability Roadmap
Identity Management Key Issues

- The health care industry has not standardized its Level of Assurance requirements for Identity Proofing and Authentication
- The lack of consistently applied methods and criteria for both identity proofing and authentication has significantly hampered the exchange of data across organizations.
- The NIST document SP 800-63-2 provides technical guidance that includes the identity proofing process and all aspects of credential management based on the OMB M-040-04 weight scale
- The ONC HIT Policy Committee (HITPC) has put significant effort into recommendations to ONC for addressing both provider and patient identity proofing and authentication issues over the last three years
  - Example: Multi-factor authentication for remote access by providers
- A recent Executive Order also pushes for alignment with NSTIC.

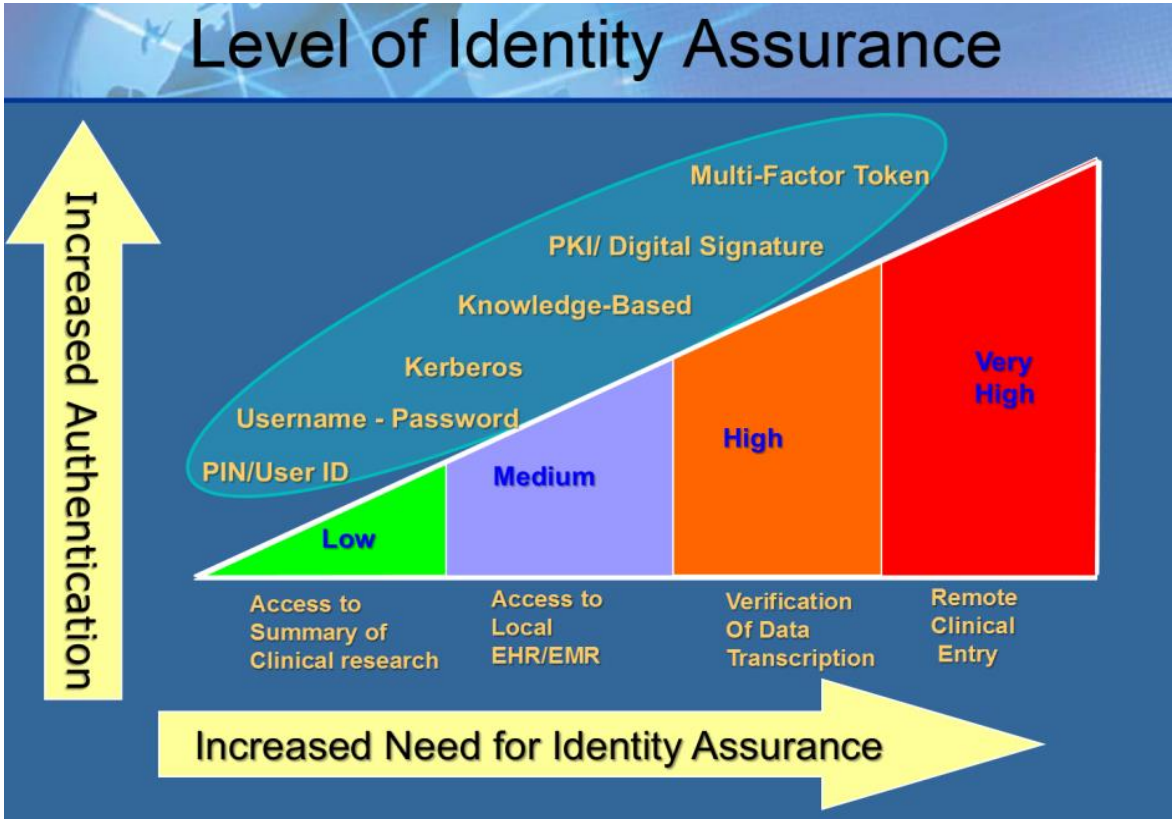
  http://www.whitehouse.gov/the-press-office/2014/10/17/executive-order-improving-security-consumer-financial-transactions

ID Proofing - NIST Electronic Authentication Guidelines 800-63-2

Putting the I in HealthIT
www.HealthIT.gov

	LOA1	LOA2	LOA3	LOA4
Verification	Unique ID in records	In person, verify picture, call or send to phone or address of record	2 documents match ; if there is no match, identity is not proven to LOA 2	Same as LOA2, visual check on both picture ID, also verify through database or govt. record
Proof by Artifacts	No requirement. Take assertion of identity at face value 	Gov't issued ID, address, DOB. If remote, bank acct, credit card, and/or tax ID 	Same as LOA2 but includes 2 forms of ID, and if remote, an utility bill with current address 	Same as LOA2 but requires 2 forms of picture ID (e.g. license and passport), a require fin acct 
Identity Claim	Must be a unique identification (not already in records)	In-person or remote presentation of credentials (presentation)	In-person or remote presentation of credentials (Verification)	In-person presentation only
	Setting up a personal email account *Gmail, Yahoo	Possessing valid government issued picture ID or financial acct # *Drivers License, Bank account number	Possess valid government issued picture ID (or financial acct #) + verification of these IDs	Possess valid government issued picture ID (or financial acct #) + verification of these IDs, + 2nd ID and verification of 2nd ID

Level of Identity Assurance



Existing Challenges in Identity Management

- Health Care has not adopted identity solutions already used in other sectors.
- Two organizations may adopted LOA levels that do not match for same role.
- Confusion
  - Is discloser liable for receiver's security failures? https://www.healthit.gov/sites/faca/files/hitpc_roadmap_transmittal_letter_2015.pdf
  - Do Security practices and standards change when new technologies take root (e.g. APIs)?
- Ensuring Identity Management *while* fostering patient engagement and self-care.

Questions