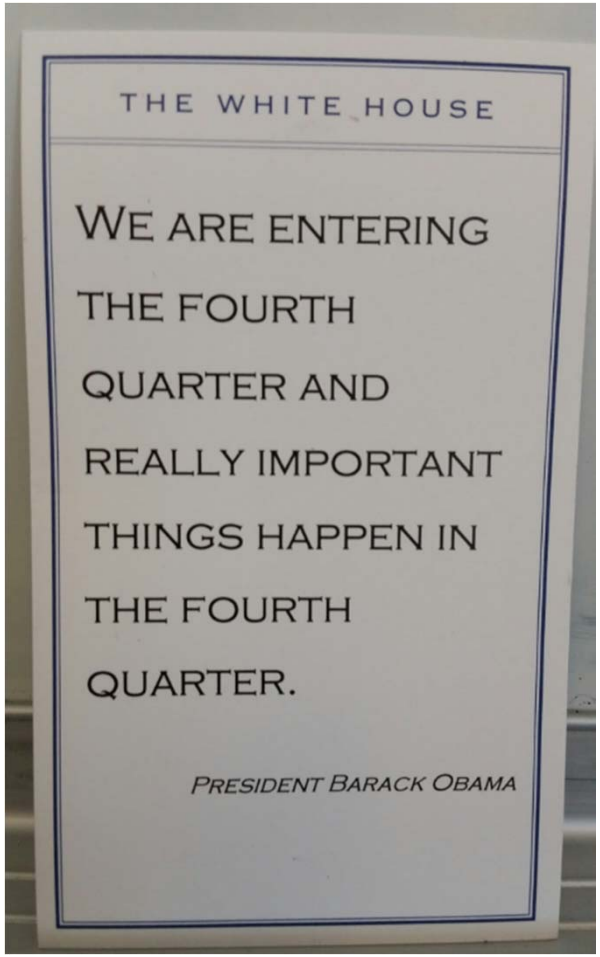
The Office of the National Coordinator for Health Information Technology

Redwood MedNet Annual Health IT Conference 2015

Building the Road to Interoperability One Section at a Time

July 31, 2015, Santa Rosa, California

Putting the I in HealthIT
www.HealthIT.gov


THE WHITE HOUSE
WE ARE ENTERING THE FOURTH QUARTER AND REALLY IMPORTANT THINGS HAPPEN IN THE FOURTH QUARTER.
PRESIDENT BARACK OBAMA

Agenda

- What is the ONC Office of the Chief Privacy Officer?
- The Road to Interoperability: Privacy & Security Issues
  - Confusion
  - Access
  - Reuse and the Learning Health System
  - Security
- Q/A

Nothing in this presentation should be construed as legal advice or official guidance.

Office of the Chief Privacy Officer

What does the Chief Privacy Officer and her Office do?

"Not later than 12 months after the date of enactment of this title, the Secretary [of HHS] shall appoint a Chief Privacy Officer of the Office of the National Coordinator [for Health IT] whose duty it shall be to advise the National Coordinator on privacy, security and data stewardship of electronic health information and to coordinate with other Federal agencies (and similar privacy offices within such agencies), with State and regional efforts, and with foreign countries with regard to the privacy, security and data stewardship of electronic individually identifiable health information."

Section 3001(e) of HITECH

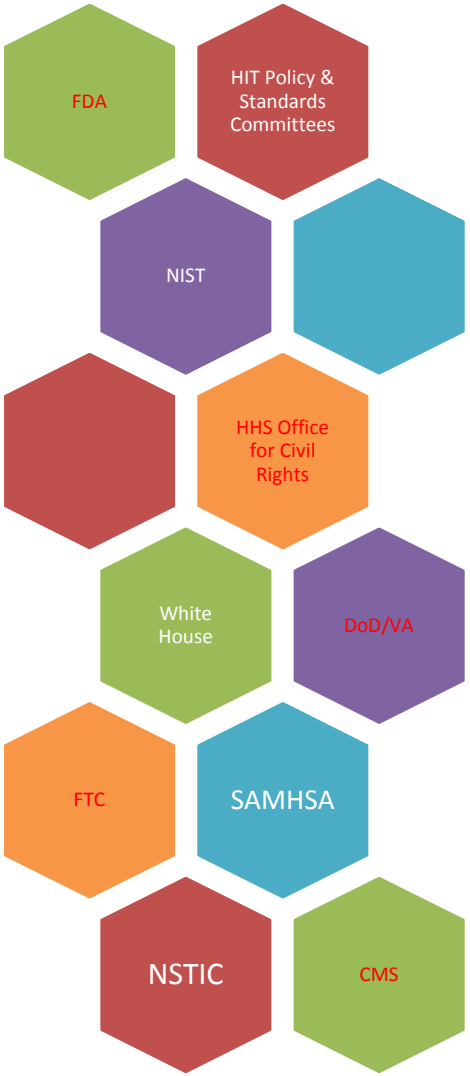
OCPO's Purpose

Strategically and proactively address the privacy and security needs of an evolving digital health information ecosystem through analysis, education, and expert advice.

OCPO's Responsibilities

Develop and coordinate privacy, security, and data stewardship policy across the federal government, state and regional agencies, and foreign countries by providing subject matter expertise and technical support

OCPO's Primary Functions



Coordinate efforts to ensure that key privacy and security protections are in place to achieve public trust in Health IT adoption, health information exchange, and meaningful use.

OCPO's Primary Functions cont'd

- Advise
- Analyze
- Educate
- Coordinate
- Solicit and listen to feedback
- Make recommendations

Across Federal Government

Within ONC and HHS

Individuals (patients and those who may become patients)

Providers and Payers

Health Information Technology Industry

OCPO's Primary Functions cont'd

Develop and provide multimedia technical assistance, toolkits, and educational materials to ONC programs, grantees and their stakeholders

Examples of OCPO Efforts (not exhaustive)

- Advise:
  - Support Health IT Policy Committee (HITECH section 3002) and Health IT Standards Committee (HITECH section 3003)
  - On Privacy and Security Standards for ONCs Certification Rules
  - Sponsor Standards & Interoperability framework activities to support P or S standards
- Coordinate:
  - Collaborate with OCR, CMS, and CDC on revised (February 2014) CLIA regulations (42 CFR 493)
  - Improving Critical Infrastructure and Cyber threat Information Sharing and Analysis efforts
- Analyze
  - mHealth (Mobile device Privacy and Security Resource Center)/Mobile Apps
  - Non-Covered Entity report to Congress (HITECH sec. 13424(b))

See Appendix for more detailed list and links to resources

OCPO as Educator

- Educate
  - Privacy & Security Guide, 2015 Edition: http://healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf
    - Cited in St. Elizabeth's settlement with OCR.
  - Model Notice of Privacy Practices
  - Tool Kits
    - Security Risk Assessment Tool
    - Downloadable privacy and security games, training videos
    - On-line resources for patient/individuals, provider, and LAWYERS.
- Solicit Feedback, Educate, Analyze, Advise, Make Recommendations
  - U.S. Big Health Data Open Government Commitment - Listening sessions December 5 & 8, 2014: http://www.healthit.gov/facas/calendar/2014/12/05/policy-privacy-security-workgroup-virtual-hearing

THE ROAD TO INTEROPERABILITY

Confusion

Draft Interoperability Roadmap states:

> Despite efforts to address potential technology standards and solutions for individual choice across this complex ecosystem, it has become clear that the complexity of the rules environment will continue to hinder the development and adoption of a consistent nationwide technical framework (e.g., data elements, definitions, vocabularies) for electronically managing individuals' basic and granular choices until the complexity is resolved.
>
> Reducing variation in the current legal, regulatory and organizational policy environment related to privacy that is additive to HIPAA will help facilitate the development of technical standards and technology that can adjudicate and honor basic and granular choices nationwide in all care settings, while ensuring that special protections that apply as a result of deliberative legislative processes remain conceptually in place. Through the course of harmonization, however, individual privacy rights as specified in state and federal laws must not be substantively eroded.

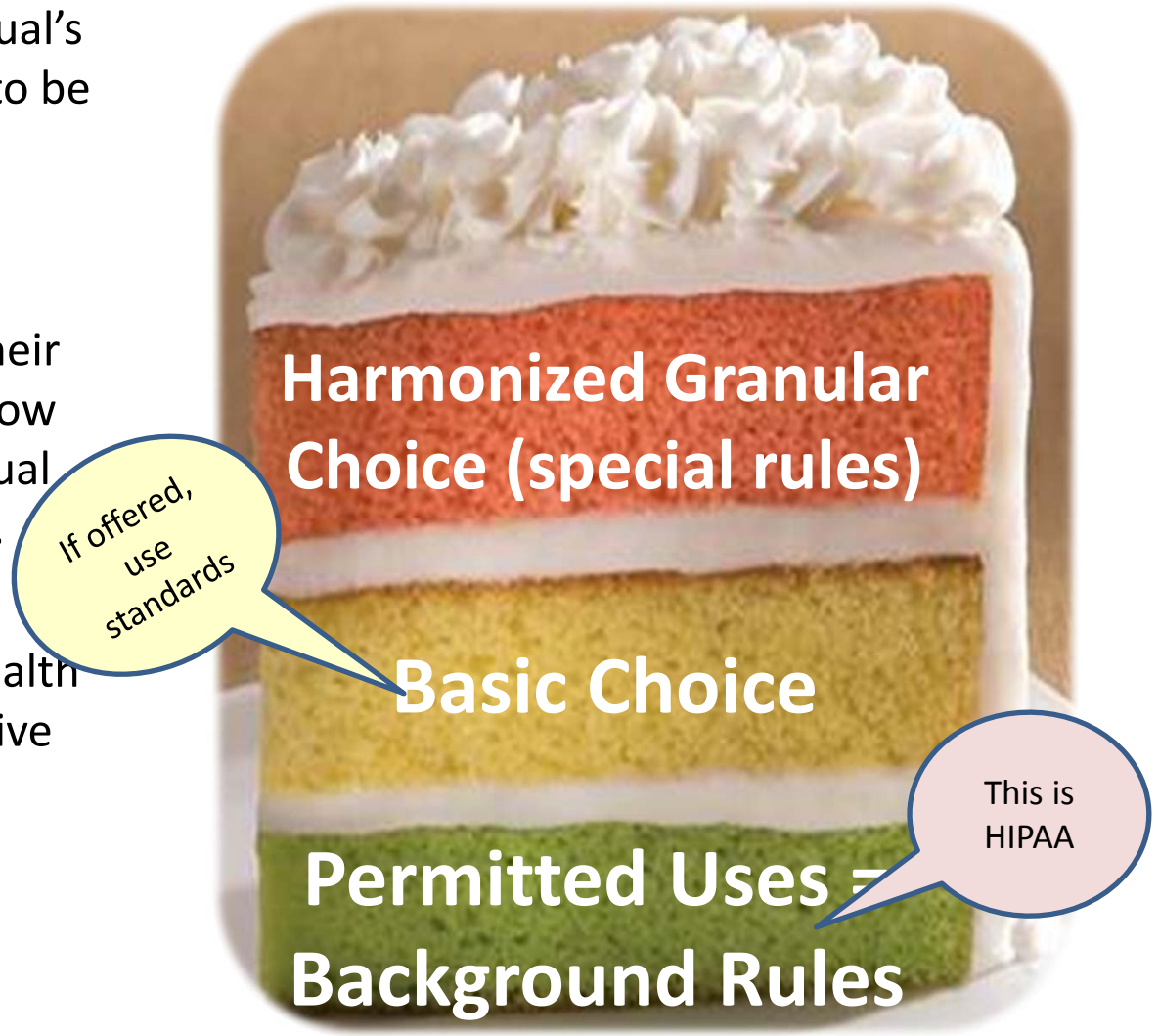
When asked whether there was confusion, PSWG said:

"Clarification from state and federal regulators (ideally with specific examples) about what is acceptable for demonstrating legal authority to access information would be enormously helpful."

https://www.healthit.gov/sites/faca/files/Appendix_C_HITPC_PSWG_Interoperability_Roadmap_Comments_2015-04-07.pdf

Goal: alleviate confusion; make it computable

- To achieve health, an individual's electronic health data need to be digitally connected to their consent choices.
- Health care providers, and their health IT systems need to know what to do when the individual does not document a choice.
- Telemedicine, community health supports, and other innovative delivery processes will be stunted if we cannot make privacy computable.



Current U.S. Privacy Rules Environment

Laws, regulations, and policies for patient consent

Laws, regulations, and policies for sensitive information

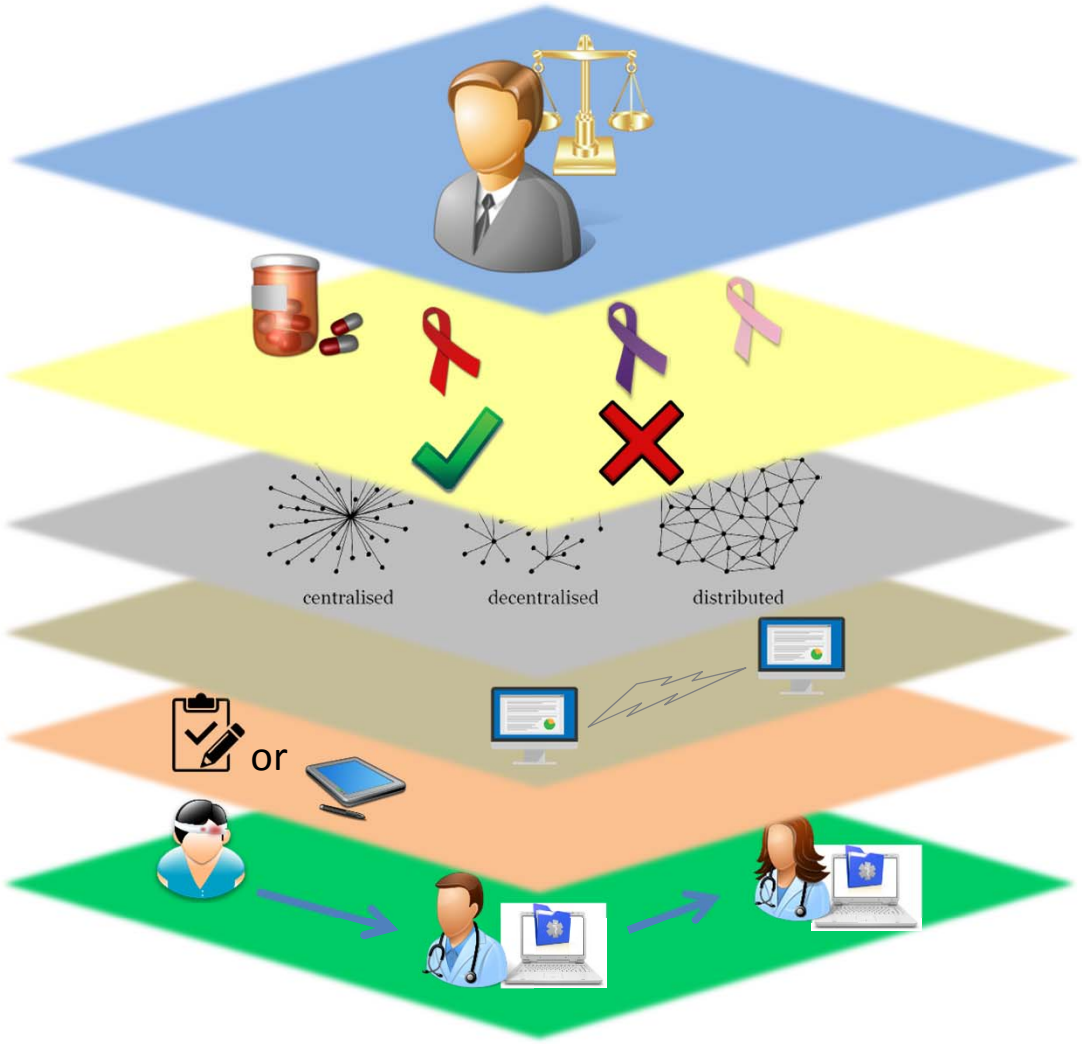
Consent models (opt-in, opt-out, with restrictions, etc.)

HIO/HIE Architecture

EHR system interoperability

Consent directive (paper/electronic)

Patient provides consent to share sensitive health information and HIPAA Permitted Uses and Disclosures



Consistent Representation of Permission to Collect, Share, and Use Identifiable Health Information

- States philosophically aligned
- State privacy and consent laws are diverse in content
- Diversity in organizational policies within states

What Others Are Saying:

CHiME
College of Healthcare Information Management Executives

Protect Patient Privacy

Challenge: Inconsistencies in consent policies and state privacy laws hinders the exchange of health information. Solution: Congress should lead an open dialogue to help states align privacy and consent policies that enable cross-border exchange of health information in a secure manner. This should include reexamining or providing clear guidance on certain provisions of HIPAA.

Achieving Interoperability that Supports Care Transformation

A Report of the American Hospital Association Interoperability Advisory Group

Providers also face significant penalties of privacy laws are broken. The multiplicity of privacy laws across state and federal governments also creates significant challenges, as do the special considerations that must be taken when sharing especially sensitive information.

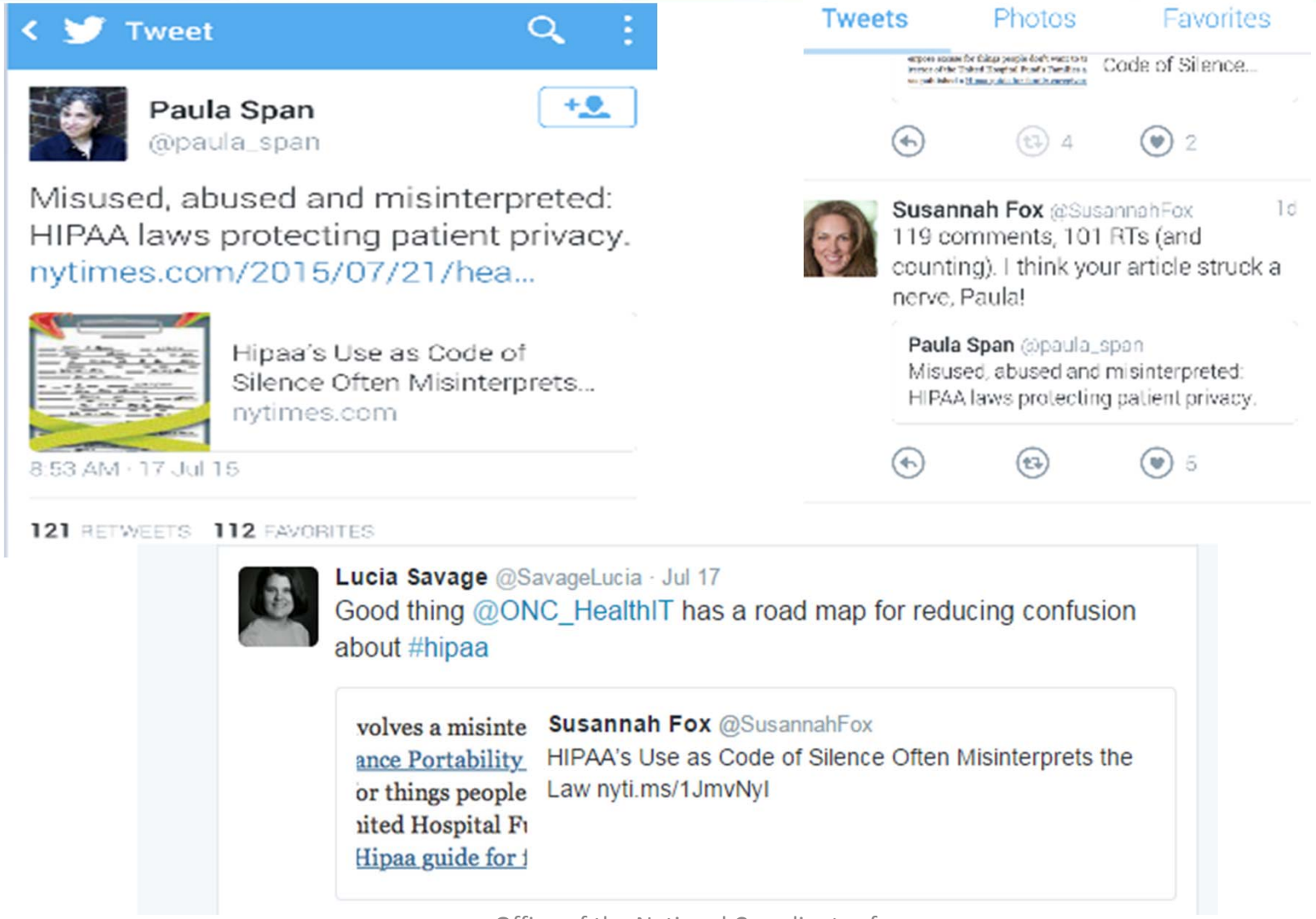
ONC's First Step towards better understanding

- Privacy & Security Guide. Page 12

Following are some scenarios to help illustrate who is and who is not a BA. This is not an exhaustive list of examples.

- You hire a company to turn your accounting records from visits into coded claims for submission to an insurance company for payment; **the company is your BA for payment purposes**.[19]
- You hire a case management service to identify your diabetic and pre-diabetic patients at high risk of non-compliance and recommend optimal interventions to you for those patients. **The case management service is a BA** acting on your behalf by providing case management services to you.
- You hire a web designer to maintain your practice's website and improve its online access for patients seeking to view/download or transmit their health information. The designer must have regular access to patient records to ensure the site is working correctly. **The web designer is a BA.**
- **Not a BA:** You hire a web designer to maintain your practice's website. The designer installs the new electronic version of the Notice of Privacy Practices (NPP) and improves the look and feel of the general site. However, the designer has no access to PHI. **The web designer is not a BA.**
- **Not a BA:** You hire a janitorial company to clean your office nightly, including vacuuming your file room. **If the janitors do not have access to PHI, then the janitors are not BAs.**

Confusion on Twitter & the New York Times.



The Road Map Plan:

1. Permitted Uses: HIPAA supports exchange for TPO
2. Make consent, when *required*, computable.
   a) Binary choices should yield similar architecture
      - In/Out of research: PMI, PCOR
3. Be more specific about when, in a HIPAA-only use case, an individuals' consent is *required*
   a) Another binary choice
   b) Learn from behavioral science
4. Specify identity control technical standards
5. Harmonize special-condition rules so they can be computable too: NAP-AX-15-004
   Interoperability Roadmap Call to Action: Alleviating and Removing Barriers to Interoperable Exchange of Data for Health Within States on www.grants.gov

45 CFR 164.524

ACCESS BY INDIVIDUALS TO THEIR OWN DATA

Access by Individuals to their health Information

http://www.wsj.com/articles/SB10001424052748703399404575395073360548340

GetMyHealthData

Patient Access and Precision Medicine

July 8, 2015

Precision Medicine Initiative: Proposed Privacy and Trust Principles

6. The success of the cohort will be enabled by the increasing ability of participants to access their own medical information. A goal of the effort will also be to provide participants access to research data in a respectful and responsible manner.

OCR and ONC Collaboration on Patient Access

The White House Announced on July 8:

New Tools for Patients: In collaboration with federal partners, the Department of Health and Human Services Office of the National Coordinator for Health IT (ONC) and Office for Civil Rights (OCR) will work to address barriers that prevent patients from accessing their health data. OCR will develop additional guidance materials to educate the public and health care providers about a patient's right to access his or her health information under the Health Insurance Portability and Accountability Act (HIPAA).

White House Precision Medicine Announcement

Look for more details on ONC Consumer eHealth Day, October 1, 2015 and following

Technology for Compliance: Data Segmentation for Privacy (DS4P)

- Proposed as optional in 2015 Edition CEHRT rule
- The DS4P standard enables interoperability and provides a capability to support existing privacy law, including federal, state, and local laws
- The standard uses document level tagging as the mechanism to convey confidentiality levels and obligations, but also specifies how to be more granular (e.g. sections or entries inside the document)
- Successfully piloted by SAMHSA for *substance use disorder* data protected by 42 CFR Part 2.

A LEARNING HEALTH SYSTEM

Other Efforts

- Identify gaps in oversight, and make recommendations, for using big health data while ensuring privacy and security.
  - On agenda for HITPC on 8/11
- Precision Medicine
  - Privacy Principles
  - Security workgroup
  - New guidance and outreach on patient access
- PCOR
  - Privacy & Security framework
  - Privacy & Security standards and technology

SECURITY & CYBER-SECURITY

Executive Order 13636 (2013) Overview

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

Presidential Policy Directive-21 (2013) Overview

PPD-21: Critical Infrastructure Security and Resilience

Develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time	Understand the cascading consequences of infrastructure failures	Evaluate and mature the public-private partnership	Update the National Infrastructure Protection Plan (NIPP)	Develop comprehensive research and development plan

*Note: The National Infrastructure Protection Plan (NIPP) 2013 was issued by DHS in response to PPD-21. It provides a clear call-to-action to leverage partnerships, innovate risk management, and focus on outcomes

Executive Order 13691 (2015) Overview

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

Cybersecurity for the Health & Public Health Sector

- The FOA EP-HIT-15-002 for the Planning Grant for Healthcare and Public Health Sector Cybersecurity Information Sharing is currently published at Grants.gov. The submission deadline is 9/14/15.
- The link to the announcement is: http://www.grants.gov/view-opportunity.html?oppId=277887

Other Security Efforts

- CEHRT Rule: Every edition raises the security bar a little bit higher
  - Many proposals in 2015 NPRM
- Security Education and Outreach
  - Security Risk Assessment tool downloaded more than 10,000 times.
- Privacy & Security Guide: Chapter 6

QUESTIONS?

The Office of the National Coordinator for Health Information Technology

Appendix:
Snapshot of Existing OCPO Educational Materials (listed alphabetically)

Office of the Chief Privacy Officer

The Office of the National Coordinator for Health Information Technology

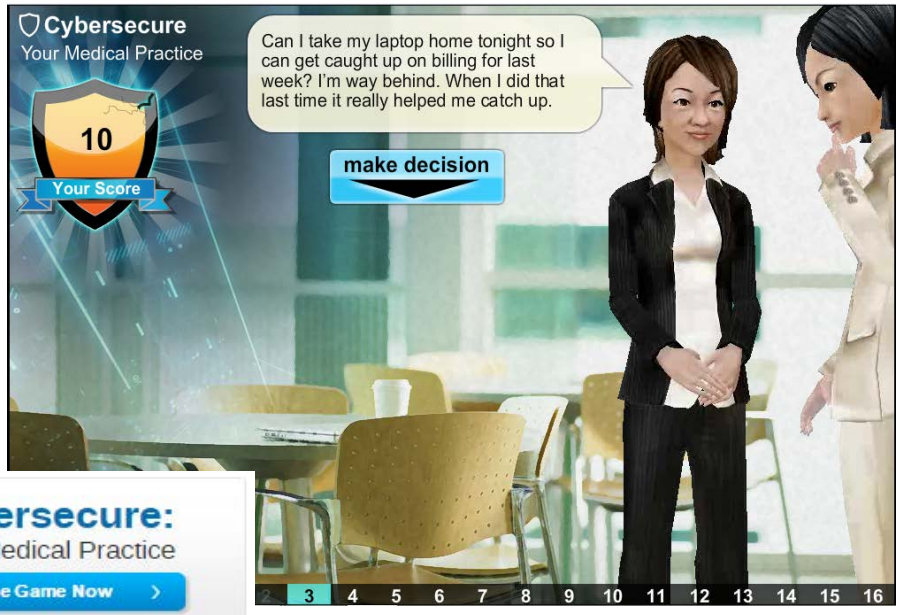
eConsent Toolkit

- **Planning Resources**
  - Practical implementation tips
  - Example patient survey
  - Focus group facilitator's guide
- **Educational Materials, Text, and Stories**
  - Interactive videos that patients viewed prior to making consent decisions
  - Non-interactive versions of the videos
  - Text for all videos
- **Technical Tools**
  - Story Engine open-source software used to create the videos
  - Architectural analysis and technical standards summary of what is needed to run Story Engine
  - Installation and user's guides for Story Engine

www.HealthIT.gov/econsenttoolkit

Cybersecure: Medical Practice

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



http://www.healthit.gov/providers-professionals/privacy-security-training-games

Cybersecure: Contingency Planning

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

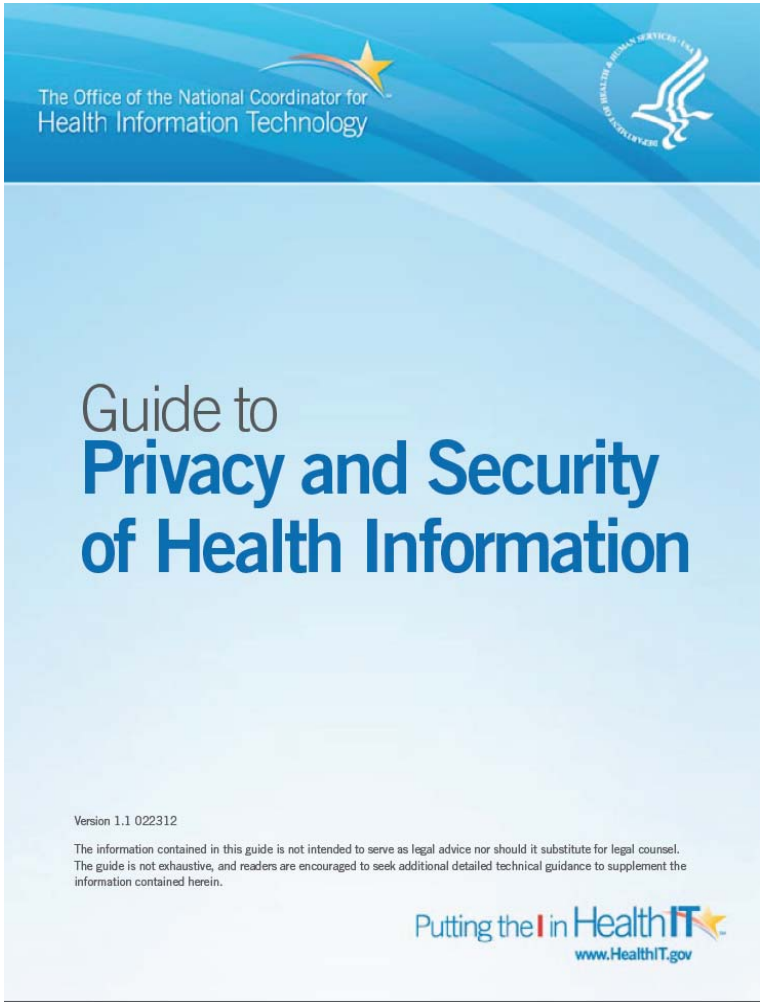
Data Segmentation for Privacy Educational Materials

Data Segmentation helps providers comply with specific state and federal laws, helping to keep the "sensitive" portions of a patient's electronic record private.

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

Guide to Privacy and Security Of Health Information – Version 1.0

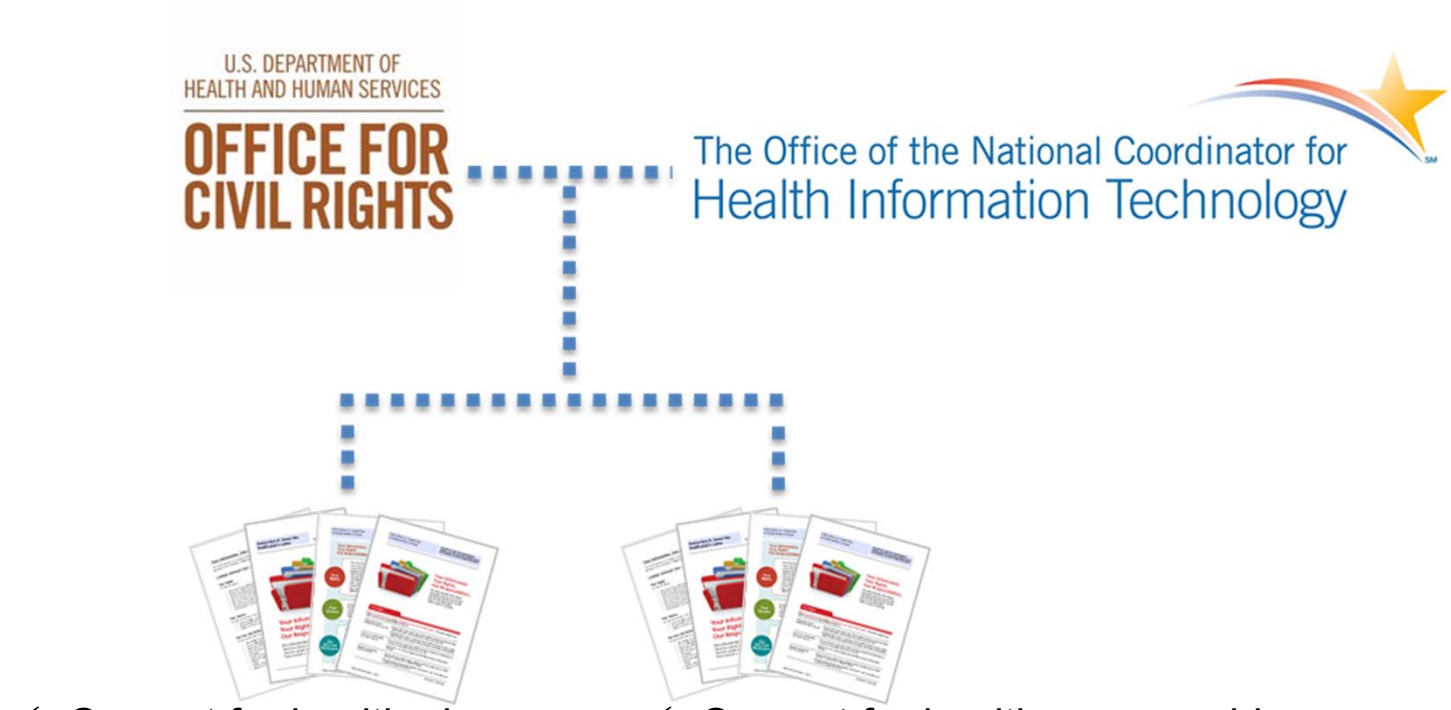
- Designed to help health care practitioners and practice staff understand the importance of privacy and security of health information at various implementation stages
- Developed with assistance from the American Health Information Management Association (AHIMA) Foundation, with input from OCR and OGC



http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

Model Notice of Privacy Practices

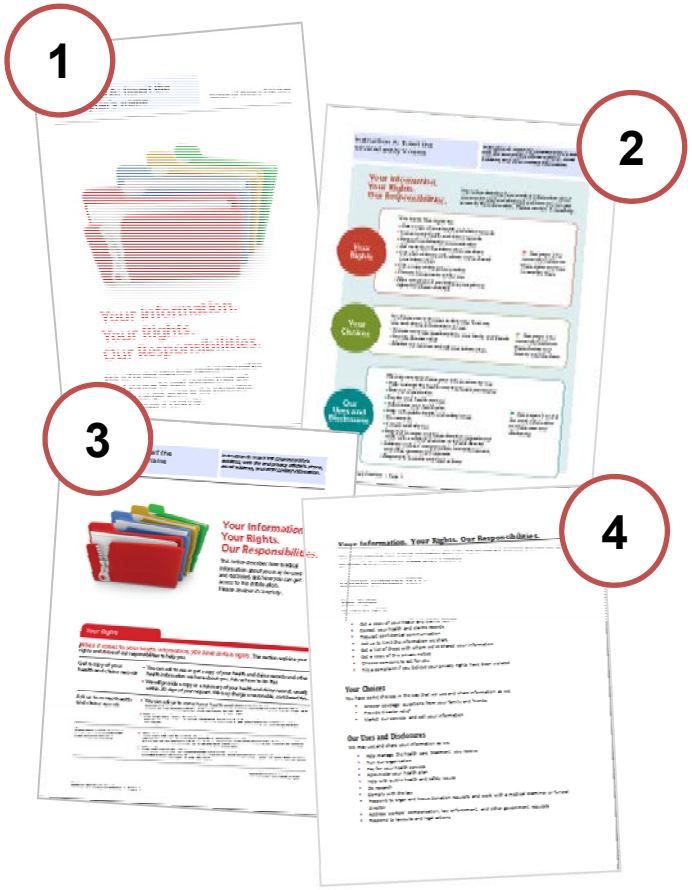
The Office for Civil Rights (OCR) and Office of the National Coordinator for Health Information Technology (ONC) collaborated to develop model NPPs for covered entities to use:



- ✓ One set for health plans
- ✓ One set for health care providers

http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html

Types of Notices Available



1. **Booklet** – Presents the material in booklet form with design elements

2. **Layered Notice** – Presents a summary of the information on the first page, followed by the full content on the following pages

3. **Full Page** – Has the design elements found in the booklet, but is formatted for full page presentation

4. **Text Only** – Provides a text-only version of the notice

http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html

Mobile Device Materials Available Online

Materials available on **HealthIT.gov/mobiledevices** include:

- Fact sheets
- Posters
- Brochures
- Postcard
- Educational videos

Protect and Secure Health Information when Using Mobile Devices

Protect and Secure health information when using mobile devices

- In a public space
- On site
- At a remote location

Regardless of whether the mobile device is:

- Personally owned, bring your own device (BYOD)
- Provided by an organization

www.HealthIT.gov/mobiledevices

OCR's YouTube Videos

Your New Rights Under HIPAA

The HIPAA Omnibus Rule

Your Health Information, Your Rights

Su Informacion de Salud, Sus Derechos

The Right to Access Your Health Information

Treatment, Payment and Health Care Operations

EHRs: Privacy and Security

Communicating with Friends And Family

Explaining the Notice of Privacy Practices

HIPAA Security Rule

http://www.youtube.com/USGovHHSOCR

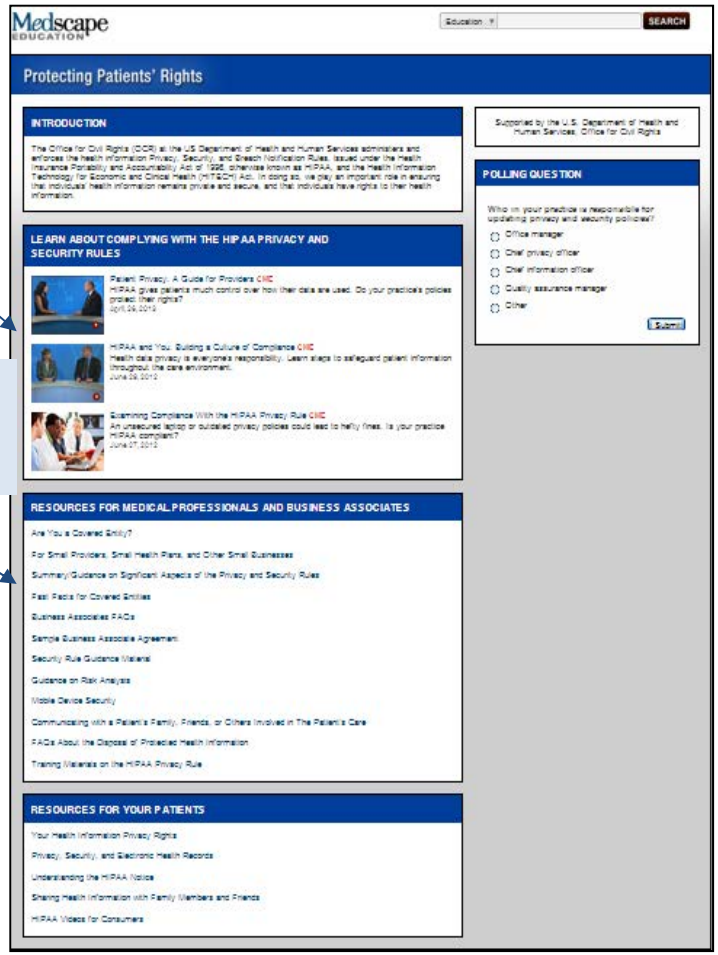
Protecting Patients Rights: OCR Resource Center @ Medscape.org

HealthIT.gov

Video Programs module imbedded into page for dynamic interest

OCR Educational Links, Including Mobile Device Content

HIPAA/OCR Poll Question Updated Quarterly



http://www.medscape.org/sites/advances/patients-rights

Security Risk Assessment Tool

- Downloadable Risk Assessment Tool designed to guide providers through the Risk Assessment process.
- The tool includes resources to
  - understand the context of the question,
  - examples of potential impacts to PHI if requirements aren't met,
  - and includes actual safeguard language from the HIPAA Security Rule

www.HealthIT.gov/security-risk-assessment

Security 101 Videos

Learn more about a risk assessment and how your practice can benefit.

Learn more about HIPAA-required contingency planning and how it helps your practice protect PHI.

www.HealthIT.gov/security-risk-assessment

Patient Resources

- **Electronic Health Records: Privacy and Security Video: https://www.youtube.com/watch?v=SMUFa5amPKs**
- **The HIPAA Omnibus Rule; Your New Rights under HIPAA; The Right to Access and Correct Your Health Information; Treatment, Payment, & Health Care Operations; Explaining the Notice of Privacy Practices; Communicating with Family, Friends and Others Involved In Your Care; HIPAA Security Rule; and Your Health Information, Your Rights Videos: https://www.youtube.com/user/USGovHHSOCR/videos**
- **Privacy, Security, and Electronic Health Records: http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/privacy-security-electronic-records.pdf**
- **Taking Charge. What to do if your identity is stolen: http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf**
- **Patient Choice: Using Technology to Enable Privacy Video: https://www.youtube.com/watch?v=yUkQNbRYuqg**
- **eConsent – Understanding a Sample Patient Experience in the eConsent Trial Project Video: https://www.youtube.com/watch?v=HCzT-YLAHWY**
- **ONC Fact Sheet on How to Keep Your Health Information Private and Secure: http://www.healthit.gov/sites/default/files/how_to_keep_your_health_information_private_and_secure.pdf**

Patient Resources

ONC Fact Sheet on How to Keep Your Health Information Private and Secure:
http://www.healthit.gov/sites/default/files/how_to_keep_your_health_information_private_and_secure.pdf

Patient Choice: Using Technology to Enable Privacy Video:
https://www.youtube.com/watch?v=yUkQNbRYuqg

eConsent – Understanding a Sample Patient Experience in the eConsent Trial Project Video:
https://www.youtube.com/watch?v=HCzT-YLAHWY

Provider Resources

- **Security Risk Assessment Tool: http://www.healthit.gov/providers-professionals/security-risk-assessment**
- **Your Mobile Device and Health Information Privacy and Security: http://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security**
- **Privacy and Security Training Games: http://www.healthit.gov/providers-professionals/privacy-security-training-games**
- **Guide to Privacy and Security of Health Information: http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf**
- **Emergency Ready – Are You Ready for Emergencies? Video: http://www.healthit.gov/emergency-ready**
- **ONC SAFER Guides: http://healthit.gov/safer/**
- **Meaningful Consent: http://www.healthit.gov/providers-professionals/patient-consent-electronic-health-information-exchange/meaningful-consent-overview**
- **Model Notice of Privacy Practices: http://www.healthit.gov/providers-professionals/model-notices-privacy-practices**
- **HIPAA Security Rule Video: https://www.youtube.com/watch?v=QWRn2r5R7ts**

Security Risk Assessment Tool:

http://www.healthit.gov/providers-professionals/security-risk-assessment

Your Mobile Device and Health Information Privacy and Security:

http://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security

Privacy and Security Training Games:

http://www.healthit.gov/providers-professionals/privacy-security-training-games

Guide to Privacy and Security of Health Information:

http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

Provider Resources

Emergency Ready – Are You Ready for Emergencies? Video:
http://www.healthit.gov/emergency-ready

ONC SAFER Guides: http://healthit.gov/safer/

Meaningful Consent: http://www.healthit.gov/providers-professionals/patient-consent-electronic-health-information-exchange/meaningful-consent-overview

Model Notice of Privacy Practices:
http://www.healthit.gov/providers-professionals/model-notices-privacy-practices

Developer Resources

- **Data Segmentation for Privacy: http://www.healthit.gov/providers-professionals/data-segmentation-overview**
- **Data Provenance Initiative: http://wiki.siframework.org/Data+Provenance+Initiative**
- **eConsent Toolkit: http://www.healthit.gov/providers-professionals/patient-consent-electronic-health-information-exchange/econsent-toolkit**