The Office of the National Coordinator for Health Information Technology

ONC Office of the Chief Privacy Officer
ONC Privacy and Security Policy Update

HIPAA Summit, Washington DC

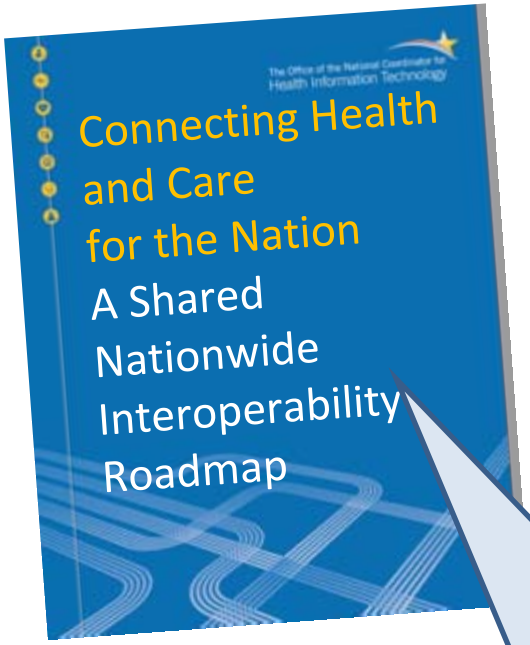
March 17, 2015

Office of the Chief Privacy Officer

The Office of the National Coordinator for Health Information Technology

HealthIT.gov

Interoperability Roadmap Released January 29, 2015



- **Interoperability (Roadmap Definition)**
  - The ability of a system to exchange information with and use information from, other systems without special effort on the part of the customer
- **Interoperability 10-year Goal**
  - Majority of providers and individuals securely send, receive, find, and use essential health information
- **Differing Legal Requirements**
  - Though legal requirements differ across the states, nationwide interoperability requires a consistent way to represent an individual's permission to collect, share, and use their individually identifiable health information, including with whom and for what purpose(s).

Comment Period Closes April 3, 2015
http://www.healthit.gov/policy-researchers-implementers/interoperability

Why Interoperability?

- Significant progress in digitizing the care experience
- Consumers increasingly expect and demand real-time access to their electronic health information
- Evolving delivery and payment models are not only driving appropriate data sharing, but depend on it
- Successes and promising practices exist and can be built on
- Technology is rapidly evolving
- Opportunities to improve care and advance science in a learning health system environment demand rapid action

DRAFT Shared Nationwide Interoperability Roadmap - Version 0.5

The Vision

Health IT Standards Committee
A Public Advisory Body on Health Information Technology to the National Coordinator for Health IT

2015 - 2017	2018 - 2020	2021 - 2024
Nationwide ability to send, receive, find, use a common clinical data set	Expand interoperable data, users, sophistication, scale	Broad-scale learning health system

Core technical standards and functions

Certification to support adoption and optimization of health IT products & services

Privacy and security protections for health information

Supportive business, clinical, cultural, and regulatory environments

Rules of engagement and governance

Functional and Business Requirements for a Learning Health System

Core technical standards and functions

1. Consistent data formats and semantics
2. Consistent, secure transport technique(s)
3. Standard, secure services
4. Accurate identity matching
5. Reliable resource location

Certification to support adoption and optimization of health IT products and services

6. Stakeholder assurance that health IT is interoperable

Privacy and security protections for health information

7. Ubiquitous, secure network infrastructure
8. Verifiable identity and authentication of all participants
9. Consistent representation of permission to collect, share, and use identifiable health information
10. Consistent representation of authorization to access health information

Supportive business, clinical, cultural, and regulatory environments

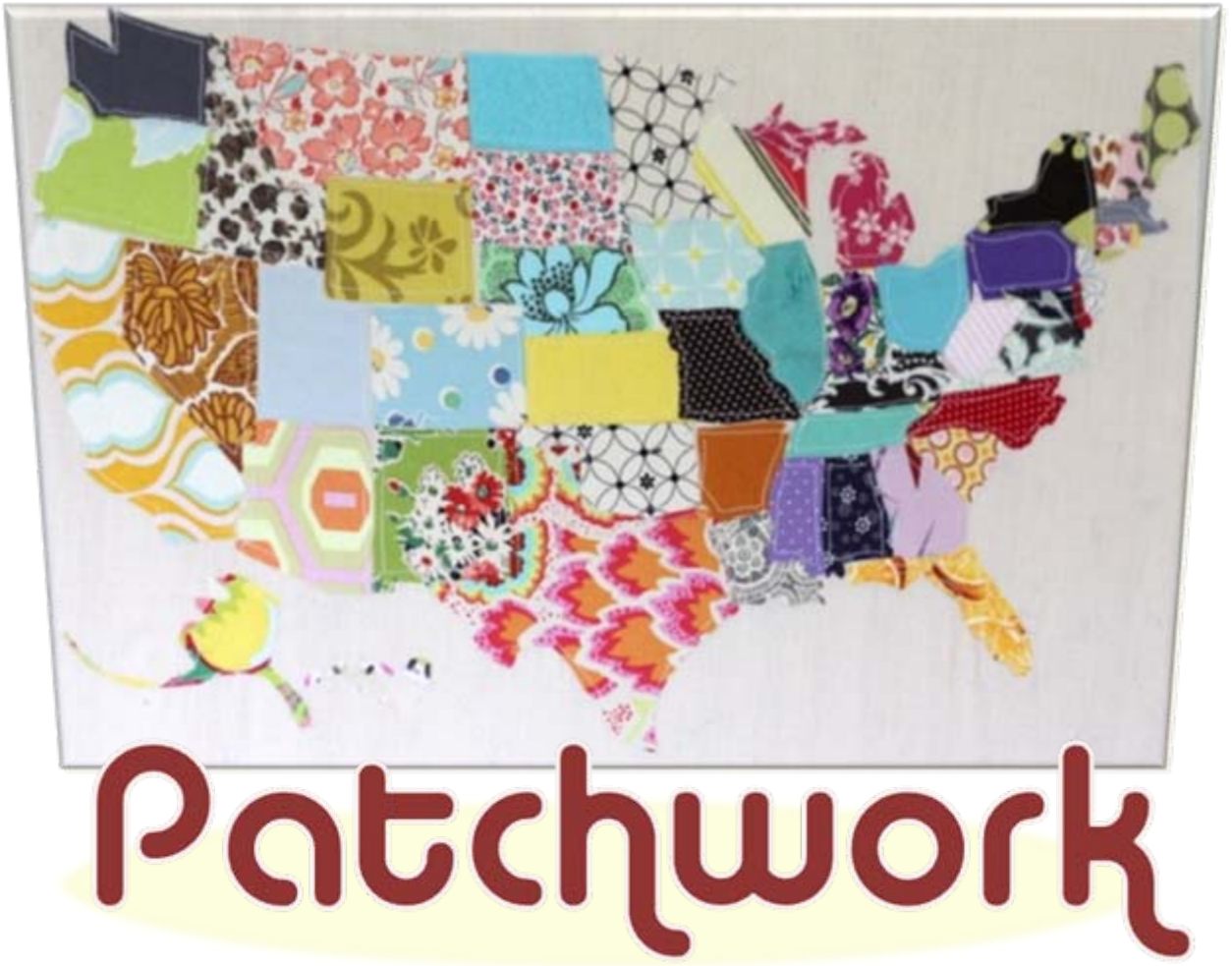
11. A supportive business and regulatory environment that encourages interoperability
12. Individuals are empowered to be active managers of their health
13. Care providers partner with individuals to deliver high value care

Rules of engagement and governance

14. Shared governance of policy and standards that enable interoperability

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
- See roadmap appendix A and B for ONC Consent Bibliography



Framing Consent/ Patient Choice Strategy

Variation in rules about permission to access, use, or disclose makes it difficult to build software systems that accurately capture, maintain, and persist this data. But we need software systems to capture and persist both written individual directions and what is permitted without a written individual direction.

Consent Management → *Evolving to* → **Computable Privacy**

Current U.S. Privacy Rules Environment

Laws, regulations, and policies for patient consent

Laws, regulations, and policies for sensitive information

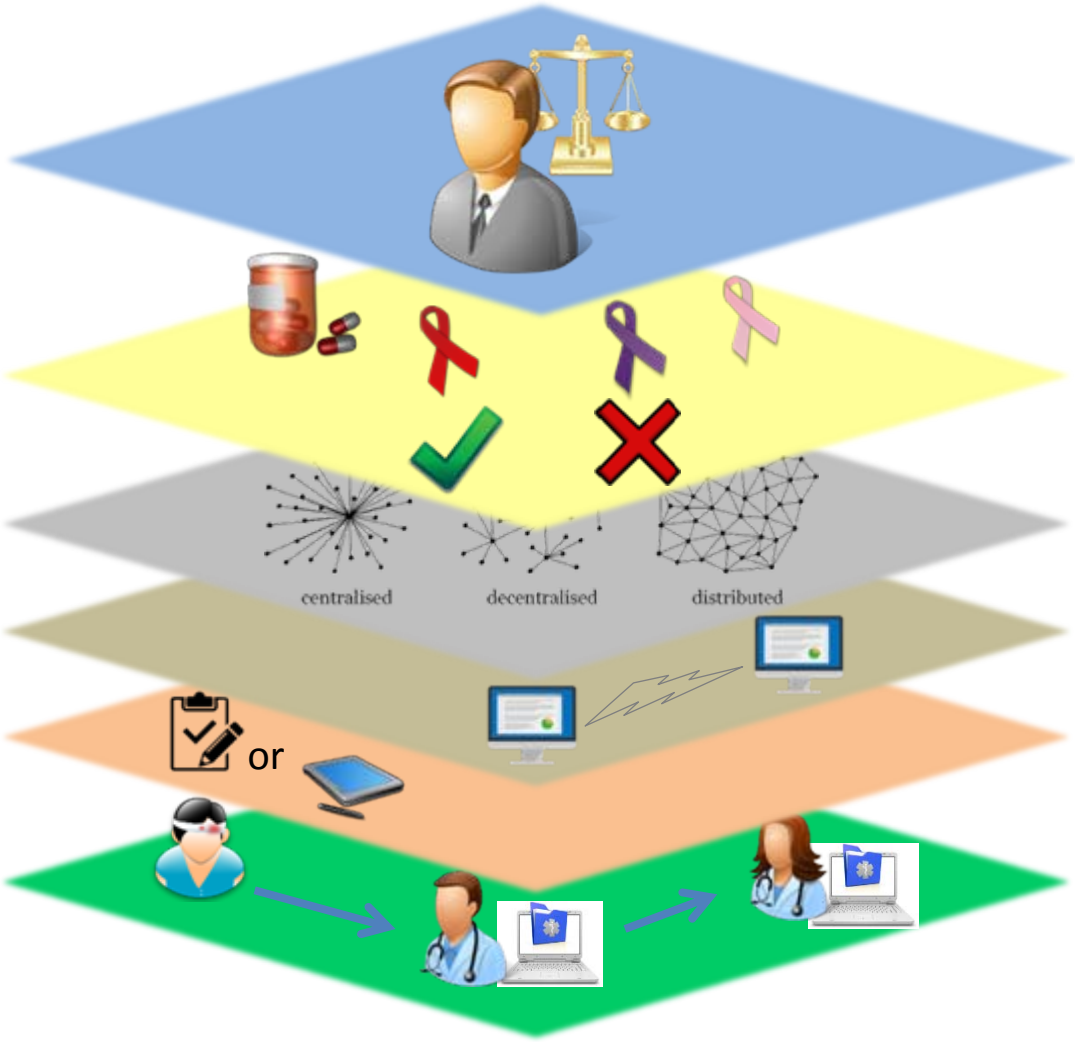
Consent models (opt-in, opt-out, with restrictions, etc.)

HIO/HIE Architecture

EHR system interoperability

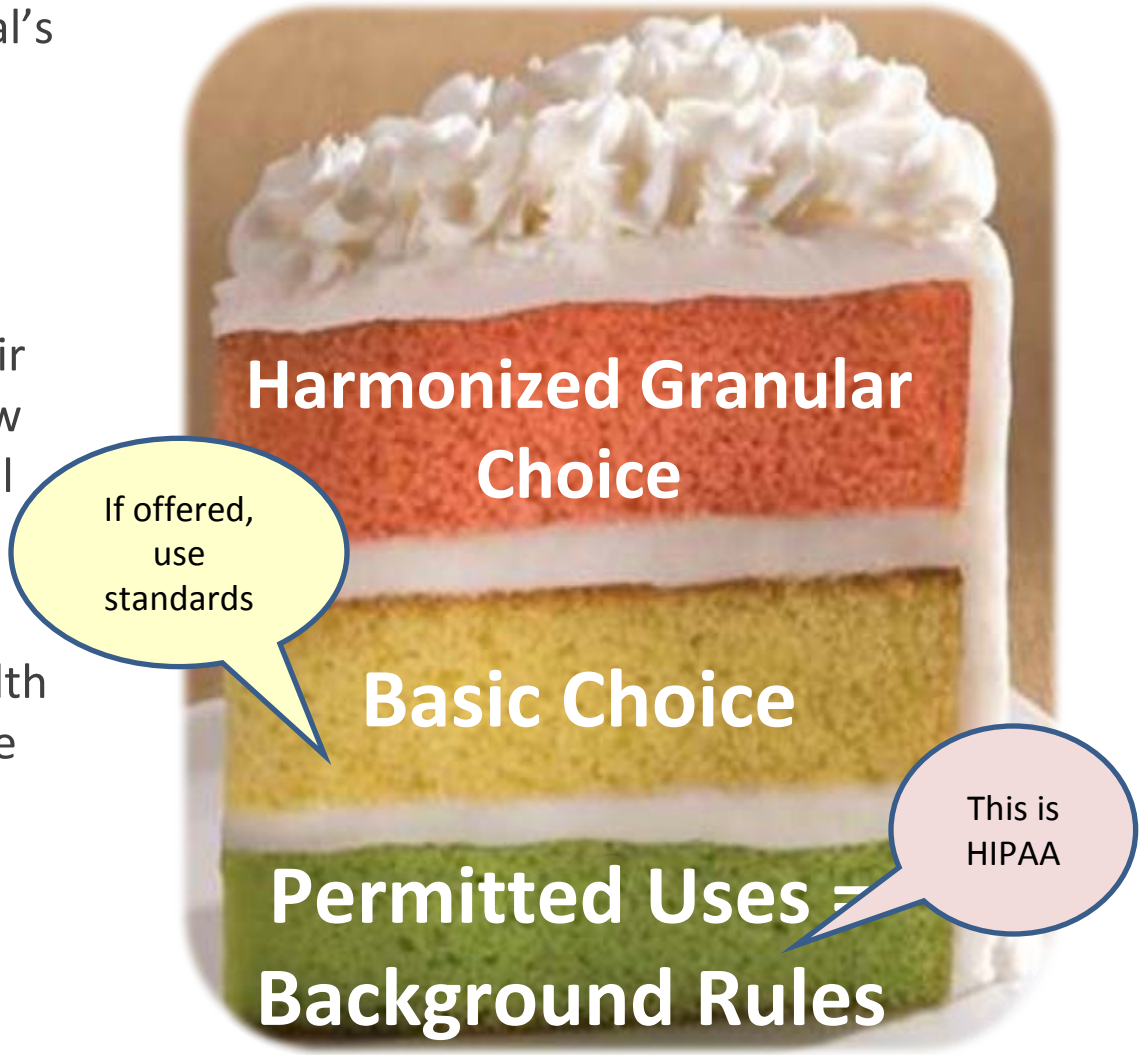
Consent directive (paper/electronic)

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



What is Computable Privacy?

- 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.



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

- **Basic Choice** = the choice an individual makes about whether their health information should be electronically exchanged; while HIPAA *does not require that choice be offered to move data for TPO*, when Basic Choice is offered, it should be offered pursuant standards.

- **Granular Choice**: the choice an individual makes to share specific types of information, including
  1. information that fits into categories to which *special legal protections* (in addition to HIPAA) apply,
     a) Clinical categories
     b) Age-based categories
  2. the choice to share health information by specific provider or payer types.

Source: Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap, DRAFT v 1.0, p. 65.

Ubiquitous, Secure Network Infrastructure

Learning Health System (LHS)Requirement

•***Ubiquitous, secure network infrastructure****:* Enabling an interoperable, learning health system requires a stable, secure, widely available network capability that supports vendor-neutral protocols and a wide variety of core services

ROADMAP SEEKS INPUT:

Cybersecurity:

•What should the federal government (specifically) focus on first to move towards a uniform approach to enforcing cybersecurity in healthcare (keeping HIPAA and CEHRT Rules in mind and possible new cybersecurity legislation)? Are there frameworks, methodologies, incentive programs, etc. that the healthcare industry has not, but should, consider?

Encryption:

•Are there other gaps (aside from lack of policies and guidance for implementing encryption)in technology and standards for encryption?

Verifiable Identity and Authentication of All Participants

LHS Requirement

- ***Verifiable identity and authentication of all participants****:* Legal requirements and cultural norms dictate that participants be known, so that access to data and services is appropriate. This is a requirement for all participants in a learning health system regardless of role (individual/patient, provider, technician, etc.)

ROADMAP SEEKS INPUT:

- What ID proofing and authentication standards, policies, and protocols can we borrow from other industries? Is healthcare *that* different from banking, social media, or email?

Source: Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap, DRAFT v 1.0, p. 58.

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

LHS Requirement

•***Consistent representation of permission to collect, share and use identifiable health information:*** Though legal requirements differ across the states, nationwide interoperability requires a consistent way to represent an individual's permission to collect, share and use their individually identifiable health information, including with whom and for what purpose(s).

ROADMAP SEEKS INPUT:

•What standards should we put forward in the 2016 standards advisory for basic choice?

•How much work should ONC be doing on other standards while clarifying permitted uses? If standards development needs to be done, what should we be working on (DS4CDS vs DS4P vs something else)?

Public Comments on Roadmap

- **Find the road map at: http://www.healthit.gov/policy-researchers-implementers/interoperability**
- **Submit your comments by 5 pm eastern on April 3 at: http://www.healthit.gov/policy-researchers-implementers/interoperability-roadmap-public-comments**

Other ONC Items—

Cool Tools to Help

- http://www.healthit.gov/providers-professionals/ehr-privacy-security
- Security Risk Assessment Tool: http://www.healthit.gov/providers-professionals/security-risk-assessment-tool
- Ten steps: http://www.healthit.gov/providers-professionals/ehr-privacy-security/10-step-plan

Questions?