The Office of the National Coordinator for Health Information Technology

Interoperability Standards for Patient Privacy

Johnathan Coleman, CISSP, Security Risk Solutions Inc.
Initiative Coordinator (Contractor) Office of the National Coordinator for Health IT

SC HIMSS, May 11, 2016

HealthIT.gov

Outline of Topics

- Current Privacy Rules Environment
- Technical Privacy Standards
- User Story Example: Data Segmentation for Privacy
- Helpful Resources

A Patchwork of Intersecting Rules

PRIVACY RULES ENVIRONMENT

Current Privacy Rules Environment

- HIPAA Privacy Rule allows health care providers to disclose protected health information without patient consent for treatment, payment and health care operations purposes.
- HIPAA leaves in place other state and federal privacy laws that are more protective.
- Some state and federal privacy laws which address social hostility and stigma associated with certain medical conditions require consent to disclose information beyond that required by HIPAA.*

*See Additional Resources included in the ***Interoperability Roadmap***
http://www.healthit.gov/sites/default/files/nationwide-interoperability-roadmap-draft-version-1.0.pdf

Current Privacy Rules Environment

Examples of Heightened Legal Privacy Protections

- **42 CFR Part 2**: Federal Confidentiality of Alcohol and Drug Abuse Patient Records regulations protect specific health information from exchange without patient consent.
- **Title 38, Section 7332, USC**: Laws protecting certain types of health data coming from covered Department of Veterans Affairs facilities and programs. Types of data include sickle cell anemia, HIV, and substance abuse information.
- **45 CFR §164.522(a)(1)(iv)**: This final rule describes how patients may withhold any health information from health plans for services they received and paid for out-of-pocket.

Separating Policy from Technical Capability

TECHNICAL PRIVACY STANDARDS

Technical Privacy Standards

Separating Policy from Technical Capability

- Standards are technical specifications to enable interoperability between communicating systems, and to provide a capability to help implement and support policies.

- Examples of Standards Development Organizations (SDOs) include:
  - Health Level 7 (HL7) International
  - Integrating the Healthcare Enterprise (IHE) International
  - OASIS
  - National Council for Prescription Drug Programs (NCPDP)
  - ASTM International

Examples of Privacy Standards

Putting the I in HealthIT
www.HealthIT.gov

Capability	Standard/Profile	Specific Usage
Data Segmentation for Privacy (DS4P)	HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1	Apply security and privacy labels to data to enable fine-grained access control
Patient Consent Structure	HL7 Implementation Guide for CDA®, Release 2: Consent Directives, Release 1 (DSTU)	Provides representations for expressing privacy preferences and exchanging privacy policies that can be enforced by consuming systems
Conveying Identity	- Cross-Enterprise User Assertion (XUA) - OASIS SAML Specification Version 2.0 - X.509 Digital Certificates	- IHE XUA Metadata - SAML Assertion (SAML Request and Response) - PKI to support Direct implementations

Using standards to protect privacy while appropriately sharing sensitive data

EXAMPLE: DATA SEGMENTATION FOR PRIVACY (DS4P)

Data Segmentation Resources and Website

Putting the I in HealthIT
www.HealthIT.gov

- 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.

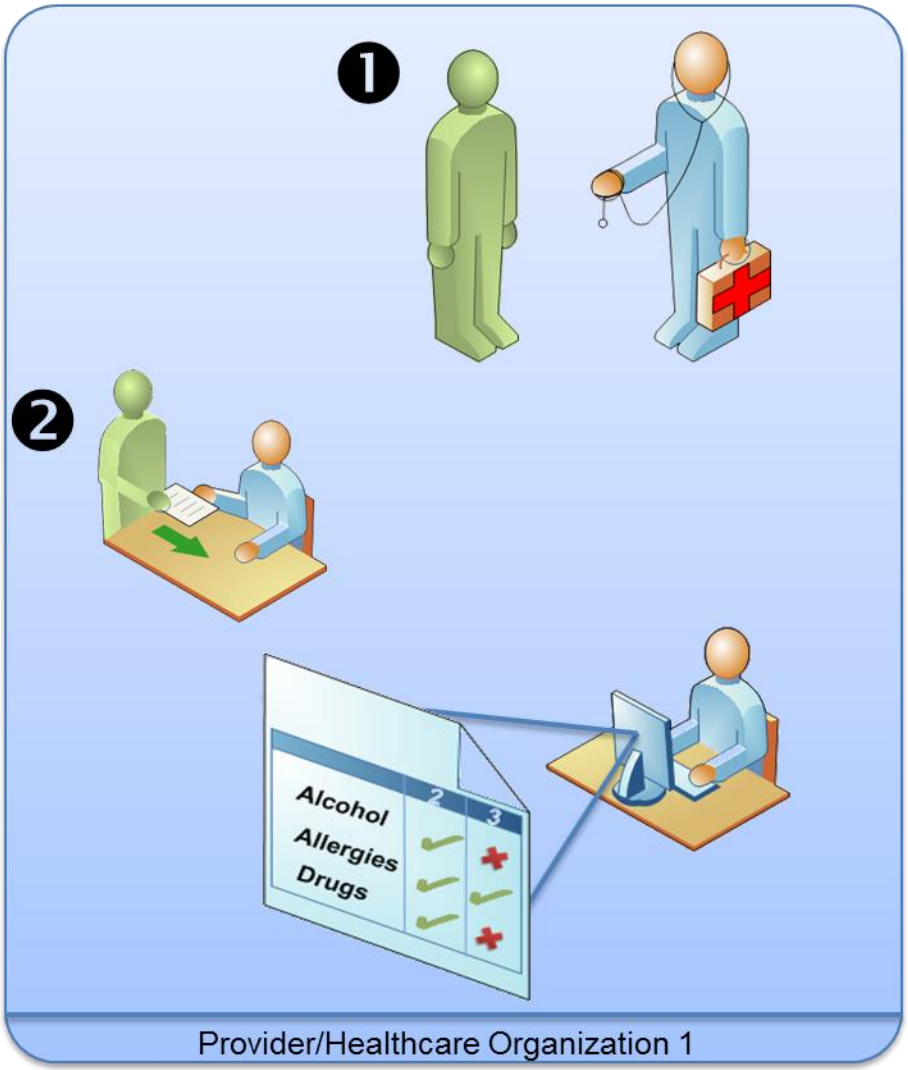
http://www.healthit.gov/providers-professionals/data-segmentation-and-you

DS4P Standards

HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1

- Voted on and approved at the highest level, to become what HL7 calls a “normative” standard, and has also received ANSI (American National Standards Institute) accreditation.
- 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) if the implementing technology can support it.
- The standard uses vocabularies to convey specific meanings, such as “Do not re-disclose without consent” or “This document is restricted”.

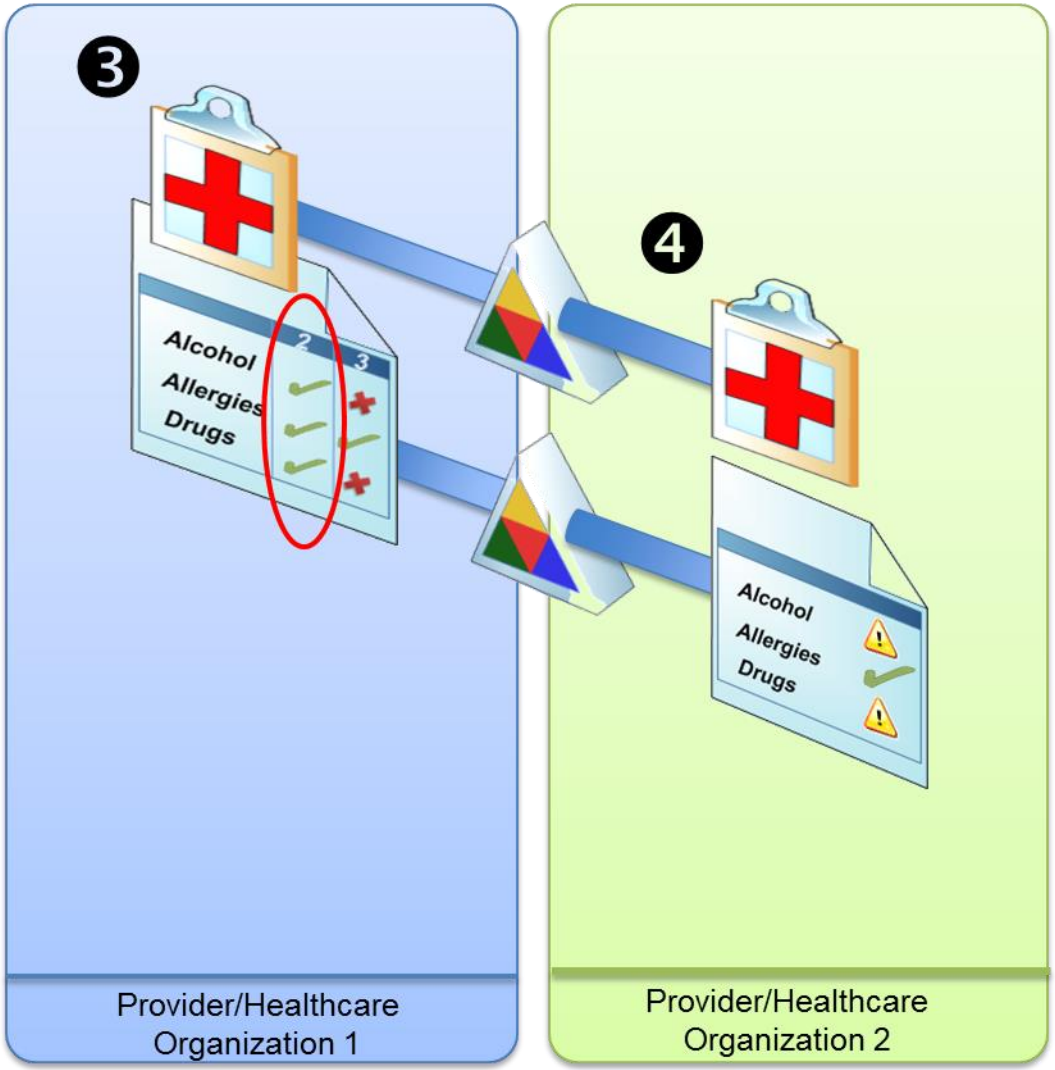
DS4P User Story Example



❶ The Patient receives care at their local hospital for a variety of conditions, including substance abuse as part of an Alcohol/Drug Abuse Treatment Program.

❷ Data requiring additional protection and consent directive are captured and recorded. The patient is advised that the protected information will not be shared without their consent.

DS4P User Story Example



❸ A clinical workflow event triggers data to be sent to Provider/Organization 2. This disclosure has been authorized by the patient, so the data requiring heightened protection is sent along with a prohibition on redisclosure.

❹ Provider/Organization 2 electronically receives and incorporates protected data, noting prohibition on redisclosure without consent.

Why is this Important?

According to estimates posted on healthit.gov:

- An estimated 26% of Americans age 18 and older are living with a mental health disorder in any given year.
- 46% will have a mental health disorder over the course of their lifetime.
- An estimated 8% of Americans are in need of drug or alcohol abuse treatment.
- Patients suffering from serious mental illness have increased rates of co-occurring conditions, which results in a reduced life expectancy of 8-17 years.

Benefits of DS4P

- Standards for data segmentation will continue to facilitate improved sharing and integration of sensitive health information among providers.

- Allowing this type of sensitive information to flow more freely to authorized recipients will give healthcare providers greater access to the patient's medical history and improve the overall quality of care.

Privacy Standards and Interoperability

HELPFUL RESOURCES

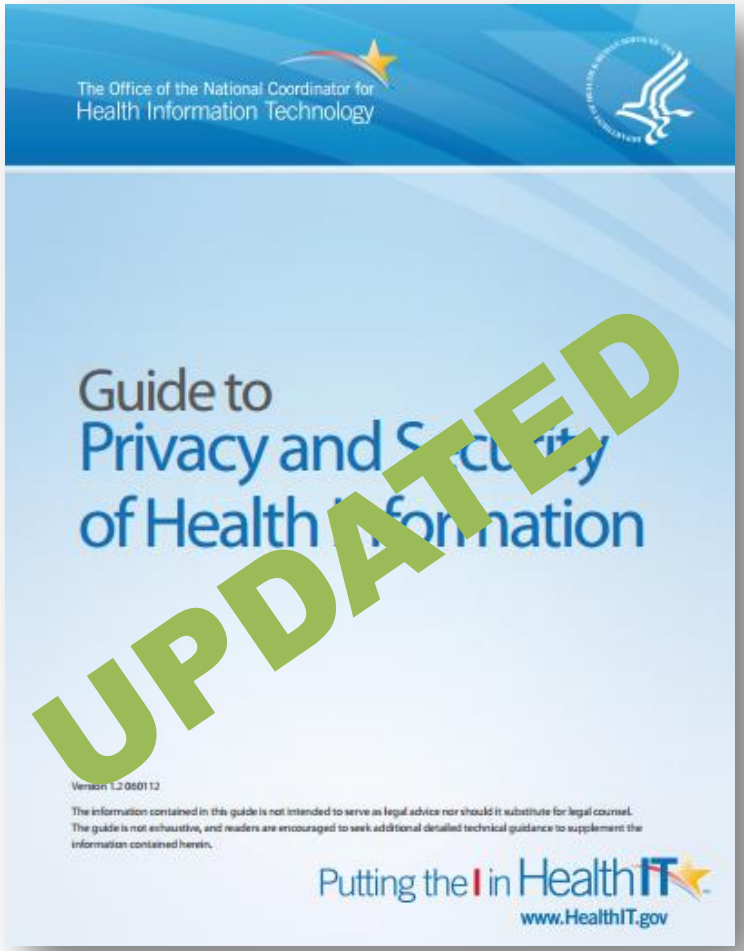
Guide to Privacy and Security Of Health Information – Version 2.0

Putting the I in Health IT
www.HealthIT.gov

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



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

Helpful Resources

- ***Interoperability Roadmap***
  https://www.healthit.gov/policy-researchers-implementers/interoperability

- ***Interoperability Standards Advisory***
  https://www.healthit.gov/standards-advisory/2016

Funding Opportunities (1)

Putting the I in HealthIT
www.HealthIT.gov

High Impact Pilots and Standards Exploration Awards Funding Opportunity Announcements

- May 9th ONC announced two cooperative agreement programs worth $1.5 million, designed to build on federal and private efforts to ensure that health information can flow where and when it is needed.
- Three to seven High Impact Pilot (HIP) projects are expected to be funded ranging from $100,000 to $500,000.
- Three to five Standards Exploration Award (SEA) projects are expected to be funded ranging from $50,000 to $100,000.

Funding Opportunities (2)

Putting the I in HealthIT
www.HealthIT.gov

ONC is Supporting NSTIC* Pilots for Federated Identity Management in Health Care

- NIST anticipates funding one award in the range of $750,000 to $1,000,000 for 18 months to demonstrate use of federated online identity solution for patients and providers across multiple health care organizations.
- More information in upcoming webinars and online:
  - May 18, 2:00-3:30pm (ET)
  - May 26, 3:00-4:30pm (ET)
  - http://nstic.blogs.govdelivery.com/2016/03/31/healthcarepilot/

**National Strategy for Trusted Identities in Cyberspace*

Thank you!

QUESTIONS?

Johnathan Coleman, CISSP
Principal, Security Risk Solutions, Inc.
Mt. Pleasant, SC 29464
Cell:(843) 442-9104
jc@securityrs.com
www.securityrisksolutions.com