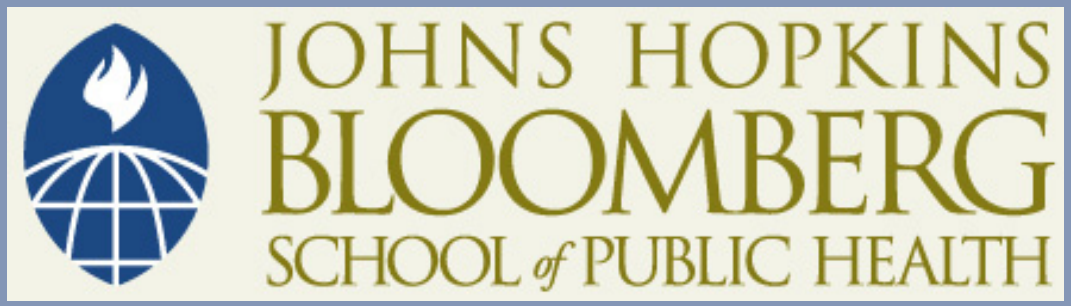

JOHNS HOPKINS
UNIVERSITY

Section C

Privacy of Health Information, Part 2

Privacy of Health Information: Current Practices

- Most consumer privacy conducted via paper forms
  - General consumer privacy consent offered at initial point of care/enrollment (when required)
  - Additional patient consent/authorization for specific health information, specific disclosure purposes (when required)
  - No standard paper consent forms within a jurisdiction (state)
    - Each organization/program has its own forms
    - Some states beginning to establish a standard form

- Most current requirements focus on uses and disclosures (including access)
  - Very little on collection of health information

Privacy of Health Information: Portability Issues

- Inter-jurisdictional portability
  - Consumer privacy consent laws and requirements, and consumer privacy desires and directives in one jurisdiction, may not be legally applicable/enforceable in another jurisdiction
    - An entity operating in one jurisdiction uses and discloses health information based on its own policies and procedures, created to meet consent requirements under that jurisdiction
    - When information is disclosed to a different entity in another jurisdiction, the receiving entity applies its own policies and procedures to the received data, which were created to meet consent requirements under the receiving entity's jurisdiction

Privacy of Health Information: Cross-Validation Issue

- Cross-validation and verification of conflicting consents
  - What is the most recent/latest consent from a patient?
  - Does that override other consents for specific data, specific purpose?
  - Where can I find the various consents issued by a consumer to perform cross-validation and verification?

Consumer Consent Options for HIEs

- **No consent:** health information of patients is automatically included—patients cannot opt out
- **Opt-out:** default is for health information of patients to be included automatically, but the patient can opt out completely
- **Opt-out with exceptions:** default is for health information of patients to be included, but the patient can opt out completely or allow only select data to be included
- **Opt-in:** default is that no patient health information is included; patients must actively express consent to be included, but if they do so, their information must be all in or all out
- **Opt-in with restrictions:** default is that no patient health information is made available, but the patient may allow a subset of select data to be included

Electronic Standards for Consumer Consent

- *A new paradigm*: offer consumers and the health care industry an interoperable, standard-based electronic mechanism to collect, capture, maintain, report, transfer, and act upon consumer consent directives, in a manner that allow users to meet different types of jurisdictional requirements

What Are Privacy Consent Directives?

- A **consent directive** is a record of a consumer's privacy policy, in accordance with governing jurisdictional and organization privacy policies, that grant or withhold consent:
  - To one or more identified entities in a defined role
  - To perform one or more operations (e.g., collect, access, use, disclose, amend, or delete)
  - On an instance or type of health information
  - For a general or specific purpose, such as treatment, payment, operations, research, public health, quality measures, health status evaluation by third parties, or marketing
  - Under certain conditions (e.g., when unconscious)
  - For specified time period (e.g., effective and expiration dates)
  - In certain context (e.g., in an emergency)

Privacy Standards for e-Health

- Main focus: consent directives
  - "The record of a healthcare consumer's privacy policy that grants or withholds consent"
  - Define the who-what-to-whom-why-when factors
  - Granular: expected to be able to handle field-level controls
  - Electronic standard: how to collect, capture, transmit, modify, reject consent directives

- Note: a common standardized "paper" consent form is not yet available but is being developed in several states

Electronic Standards for Consumer Consent

- Key characteristics
  - Consumer-friendly mechanism
    - To allow consumer to manage their consent directives electronically in a simple, reliable, secure, efficient, and effective manner
  - Scalable
    - Allow to go from general (overall opt-in/opt-out) to granular (specific data, specific people, specific people)
  - Codifiable
    - Uses standard codes to express consent directives
  - Machine-readable/machine-actionable
    - Does not require human intervention to process
    - Allow systems to operationalize access, use, and disclosure controls

Electronic Standards for Consumer Consent

- Key characteristics
  - Portable/transferable
    - Can be electronically ported/transferred between organizations and across jurisdictions
  - Flexible/adaptable
    - Features can be ‘turn-on’ or ‘turn-off’ based on differing levels of jurisdictional requirements
  - Valid/verifiable/auditable
    - Supports digital signature, non-repudiation, audit controls
  - Unambiguous/completeness
    - Conflicts between directives can be identified and resolved

Privacy Standards for e-Health

- HITSP established the interoperable standard for capturing, managing and communicating e-Consent

- Two complementary electronic standard components
  - Basic Patient Privacy Consent (BPPC)
    - Mechanism to capture and communicate consent directives in a document-based environment
  - HL7 Privacy Consent Messaging Specifications
    - Data Consent, Confidentiality Codes, Health Care Permission Catalogue

- HITSP documented standards in two products
  - HITSP Transaction Package 30 (TP30)
  - HITSP Capability 143 (CAP 143)

Consumer Preference and Consents Capability

- Capability addresses management of consumer preferences and consents as an acknowledgement of a privacy policy

- Capability is used to capture a patient/ consumer agreement to one or more privacy policies; where examples of a privacy policy may represent consent, dissent, authorization for data use, authorization for organizational access, or authorization for a specific clinical trial


November 9, 2009
Version 0.0.1

HITSP Manage Consumer Preference and Consents Capability

HITSP/CAP143

HITSP

Healthcare Information Technology Standards Panel

Submitted to:

Healthcare Information Technology Standards Panel

Submitted by:

Capabilities Team

REVIEW COPY

HITSP Manage Consumer Preference and Consents Capability
Review Copy
20091109 V0.0.1

Source: http://www.hitsp.org

Consumer Preference and Consents Capability

- TP30:
  - Describes the messages needed to capture, manage, and communicate rights granted or withheld by a consumer to one or more identified entities in a defined role to access, collect, use, or disclose individually identifiable health information (IIHI)
  - Supports the delegation of the patient's right to consent
  - Uses IHE's BPPC and supports HL7 Confidentiality Codes


November 9, 2009
Version 0.0.1

HITSP Manage Consumer Preference and Consents Capability

HITSP/CAP143

HITSP

Healthcare Information Technology Standards Panel

Submitted to:

Healthcare Information Technology Standards Panel

Submitted by:

Capabilities Team

REVIEW COPY

HITSP Manage Consumer Preference and Consents Capability
Review Copy
20091109 V0.0.1

Source: http://www.hitsp.org

Summary

- Privacy continues to be the pivotal building block of health IT and health information exchange
- Much work has been done to understand the policy commonalities and differences across federal and state jurisdictions
- More recently, the focus has been on how (and what) technology exists or is needed to support policy options
  - Including standards for content, messaging, and exchange of consumer choices
- While standards exist to support some of the current policy options, more work is needed in moving those standards into operational implementation in EHRs and HIEs