Department of Health & Human Services
Office of the National Coordinator for
Health Information Technology

Update on Privacy and Security Activities

for

National Committee on Vital and Health Statistics

February 9, 2011

Joy Pritts, J.D.
Chief Privacy Officer

HITPC Privacy and Security Recommendations on Provider Authentication

All entities involved in health data exchange should be required to have digital certificates – Examples of these entities might include:

- Covered entities (health care providers)
  - Retail pharmacies
  - Laboratories
- PHR providers
- Public health entities
- PBMs

Provider Authentication Recommendations

Organizations seeking digital certificates must demonstrate that:

- **They exist as a legitimate business (or a valid business entity)**
- **They participate in electronic health care information exchange transactions**
- **Credentialing organizations/certificate issuers should rely on existing criteria and processes when applicable – e.g., NPI**

Provider Authentication Recommendations

- Multiple credentialing entities will be needed to support issuance of digital certificates given the number of health care entities that will require them – For example, vendors and state agencies, HIOs might be authorized to issue certificates
- Should also leverage existing processes such as the Federal Bridge

Provider Authentication Recommendations

- We recommend that ONC establish an accreditation program for reviewing and authorizing certificate issuers

This requirement for accreditation should be evaluated in the context of recommendations from the HIT Policy Committee's Governance Workgroup

Provider Authentication Recommendations

- ONC, through the Standards Committee, should select or specify standards for digital certificates (including data fields) in order to promote interoperability among health care organizations.
- EHR certification should include criteria that tests capabilities to retrieve, validate, use, and revoke digital certificates that comply with standards

Patient Information Matching

- Hearing in December 2010
- Internal data collection –good starting point
- Research required to establish metrics for acceptable level of matching data to correct patients

HIT Policy Committee P&S Tiger Team

Next steps

- Provider authentication (human user level)
  - What level of assurance is appropriate under what circumstances?

- Patient ID management
  - Patient access to electronic health informati

HIT Policy Committee: Data segmentation recommendations follow up

- ONC is funding projects with respect to providing more granular choice for sharing patient information
- Focus is on behavioral health
- Working closely with SAMHSA and ONDCP

Affordable Care Act

- Enrollment workgroup-privacy and security taskforce
  - Three states as innovators –target 2013 livedate
  - Patient identity management
- Accountable care organizations—privacy issues

Personal Health Records

- **Workshop completed December 2010**
- **Study is in second draft**
- **Report to Congress with recommendations**
  - Later this year

Federal Privacy Initiatives

- **Dept. of Commerce**
  - Green paper
  - Fair Information Practices for all who transmit identifiable information over the internet
  - Voluntary industry standards
  - Response to EU Directive updates

- **FTC Framework**

  Medical Identity Theft guidance

HHS Regulatory Agenda (Federal Register 2010)

- **NPRM Individual Access to Protected Health Information Held by CLIA Laboratories**
- **Final Rules**
  - Breach Notification
  - HITECH modifications to HIPAA Privacy, Security and Enforcement
  - GINA

Questions?