Connecting America for Better Health

The Office of the National Coordinator for Health Information Technology

ONC
Update on Privacy and Security Activities

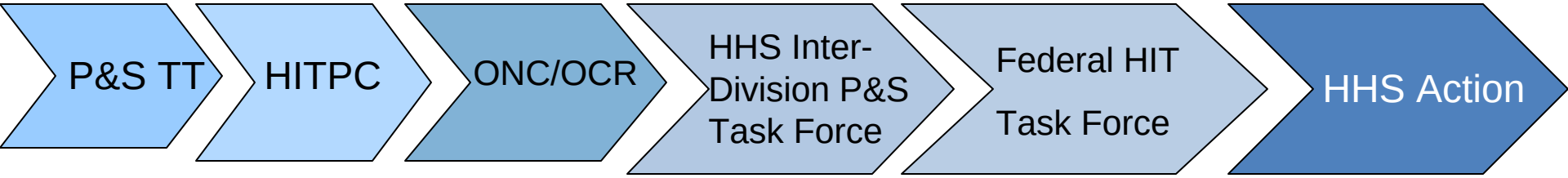
The National HIPAA Summit
March 27, 2012

Joy Pritts, JD
Chief Privacy Officer

Chief Privacy Officer Mandate

- Position created in HITECH/ARRA
- Duties:
  - *Advise* the National Coordinator on privacy, security, and data stewardship of electronic individually identifiable health information and
  - *Coordinate* with other Federal agencies. . . with State and regional efforts, and with foreign countries with regard to these efforts.

HITPC Privacy Policy Recommendations Process



HITPC Privacy Policy Recommendations Process

HHS action on recommendations. Deliberate and then

- Accept
- Reject
- Modify
- Table

HHS Potential Action Levers

- Guidelines for ONC-funded programs (e.g., Regional Extension Centers; State Health Information Exchange) requirements
- Funding requirements
- Formal Guidance
- Regulations
- Legislation

Privacy and Security Guiding Principles

- *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information*
- Based on the Fair Information Practice Principles
  - Individual access
  - Correction
  - Openness and transparency
  - Individual choice
  - Collection, use and disclosure limitation
  - Data quality and integrity
  - Safeguards
  - Accountability

Today's Focus: Recent Developments

- ONC – State HIE Program Information Notice
- Coordinated activities with CMS

State HIE Cooperative Agreements:
Program Information Notice on Privacy & Security

- Issued March 22, 2012
- Provides additional direction to states and State Designated Entities on privacy and security frameworks required as part of grantee strategic and operational plan updates
- http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_0_5545_1488_17157_43/http%3B/wci-pubcontent/publish/onc/public_communities/_content/files/onc_hie_pin_003_final.pdf

State HIE Cooperative Agreements: PIN on Privacy & Security

- Builds on recommendations of the Health IT Policy Committee as well as the *Nationwide Privacy and Security Framework*
- Some key aspects follow

State HIE Program Information Notice (PIN) Individual Access & Correction

Where HIE entities store, assemble or aggregate individually identifiable health information (IIHI), such as longitudinal patient records with data from multiple providers, HIE entities should make concrete plans to give patients electronic access to their compiled IIHI and develop clearly defined processes:

- For individuals to request corrections to their IIHI and
- To resolve disputes about information accuracy and document when requests are denied.

State HIE PIN
Individual Choice

- Where HIE entities serve solely as information conduits for directed exchange of IIHI and do not access IIHI or use IIHI beyond what is required to encrypt and route it, patient choice is not required beyond existing law.

- Such sharing of IIHI from one health care provider directly to another is currently within patient expectations.

State HIE PIN
Individual Choice (cont'd)

- Where HIE entities store, assemble or aggregate IIHI beyond what is required for an initial directed transaction, HIE entities should ensure individuals have *meaningful choice* regarding whether their IIHI may be exchanged through the HIE entity.

- This type of exchange will likely occur in a query/response model or where information is aggregated for analytics or reporting purposes.

State HIE PIN Individual Choice (cont'd)

Both opt-in and opt-out models are acceptable means of obtaining patient choice so long as choice is *meaningful.*

- Made with advance knowledge/time;
- Not used for discriminatory purposes or as condition for receiving medical treatment;
- Made with full transparency and education;
- Commensurate with circumstances for why IIHI is exchanged;
- Consistent with patient expectations; and
- Revocable at any time.

State HIE PIN
Individual Choice (cont'd)

- Individuals should have choice about which providers can access their information.

- Grant recipients are encouraged to develop policies and technical approaches that offer individuals more granular choice than having all or none of their information exchanged.

State HIE PIN

Collection, Use and Disclosure Limitation

- Providers requesting or accessing IIHI by electronic means for “treatment” generally should have or be in the process of establishing a treatment relationship with the patient who is the subject of the requested information.

- The means of verifying whether such a relationship exists could include attestation or artifacts such as patient registration, prescriptions, consults, and referrals.

State HIE PIN Safeguards

- Encryption. HIE entities should provide for the exchange of already encrypted IIHI, encrypt IIHI before exchanging it, and/or establish and make available encrypted channels through which electronic health information exchange could take place.

State HIE PIN Safeguards

- HIE entities should establish strong identity proofing and authentication policies for user access to electronic health information systems.
- Recipients should indicate the assurance level they are using in their privacy and security frameworks, using NIST 800-63 version 1.0.2 as a guide and resource.
- The recommended level of assurance is Level 3.

Beyond the Program

- Encouraging use of PIN beyond program to state policy leaders and other stakeholders working diligently to establish common privacy and security policies and practices for communities, regions and states to enable provider and public trust and support rapid progress in health information exchange.

ONC: Supporting Initiatives

- e-Consent Project
  - Exploring ways to electronically obtain meaningful consent to share information through a HIE
  - Data Segmentation Initiative
    - Standards and Interoperability Framework
    - Standards for privacy policies and individual choices

Other HHS Privacy & Security

- Stage 2 Meaningful Use and certification criteria for qualified electronic health records
- CMS Affordable Care Act Regulations
  - Availability of Medicare Data for Performance Measurement (Qualified Entities)
    - Must have a rigorous data privacy and security program
    - Data use agreement
  - Accountable Care Organizations
    - Individuals may opt out of having certain information shared

Health Insurance Exchange Rule Privacy and Security

- Patient Protection and Affordable Care Act: Establishment of Exchanges and Qualified Health Plans Final Rule
  - To be published in Federal Register March 27, 2012

- State health insurance exchanges must establish and implement privacy and security standards that are consistent with the Fair Information Practice Principles.
  - 45 CFR 155.260

The End