The Office of the National Coordinator for Health Information Technology

ONC Privacy and Security Policy Update

NCVHS
February 27, 2013

Scott Weinstein, JD
Office of the Chief Privacy Officer

Putting the I in HealthIT
www.HealthIT.gov

Introduction to the Office of the Chief Privacy Officer (OCPO)

- HITECH/ARRA created Chief Privacy Officer position

- 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.*

OCPO Responsibilities: Privacy and Security

- Policy development
  - coordination and outreach across HHS, federal government, states, and international community
  - Ensure key privacy/security protections in place to achieve public trust in HIT
  - Support goals of the Patient Protection and Affordable Care Act (ACA)
- Programmatic support
  - Provide privacy/security support to ONC programs (e.g., HIEs)
  - Serve as privacy/security expert for other HHS programs, as needed
- Research & policy implementation

OCPO – Policy Development

- Play a lead role in privacy and security-related coordination across the department, federal government and internationally:
  - HITPC Privacy and Security Tiger Team
  - HITSC Privacy and Security Work Group
  - HHS Inter-Division Privacy and Security Policy Task Force
  - Federal Health IT Interagency Privacy & Security Task Force (Cybersecurity & Privacy Subgroup)
  - National Science & Technology Council (NSTC), Subcommittee on Privacy and Internet Policy (Cabinet-level council) (EU OECD)
  - National Strategy for Trusted Identities in Cyberspace (NSTIC)
  - OMB Health IT Work Group
  - HHS Privacy Committee
  - Federal CIO Council (Federal Identity and Access Management Subcommittee - Federal Integration Working Group)

OCPO - Current Issues

- New issues before the HITPC Privacy & Security Tiger Team
  - Query/Response

- Meaningful Use Stage 3 Request for Comments
  - Summary of comments re: consent

- OCPO Project updates

HITPC Privacy & Security Tiger Team

- Developing recommendations on issues around Query/Response
  - Background - except in circumstances where the law expressly requires disclosure, the rules *permit but do not require* providers to release PHI in a range of circumstances (treatment, payment, & operations, for example).
  - Goal is to reduce potential real or perceived barriers – such as through clarification regarding provider liability for responding to a query – to enable him/her to respond to queries consistent with his/her professional obligations and the law
  - Mapping out scenarios to achieve goal:
    - Scenario 1 – Targeted Query for Direct Treatment (HIPAA controls)
    - Scenario 2 – Targeted Query for Direct Treatment, Data covered by more stringent privacy law
    - Scenario 3 – Non-targeted query

Meaningful Use Stage 3 RFC - Summary of Comments on Patient Consent/Data Segmentation

MU4: Some federal and state health information privacy and confidentiality laws, including but not limited to 42 CFR Part 2 (for substance abuse), establish detailed requirements for obtaining patient consent for sharing certain sensitive health information, including restricting the recipient's further disclosure of such information. ***Three questions were put forth.***

- 74 comments received
- ***<u>Question 1:</u> How can EHRs and HIEs manage information that requires patient consent to disclose so that populations receiving care covered by these laws are not excluded from health information exchange?***
  - Approaches suggested include:
    - Metadata tagging
    - Data segmentation , such as…
      - Data Segmentation for Privacy Initiative
      - VA/SAMHSA
      - SATVA
  - Concerns expressed:
    - The necessary segmentation capabilities do not exist today
    - It is better to focus on identifying and punishing inappropriate use of data
    - Use PHR to give patients control of their data

Meaningful Use Stage 3 RFC - Summary of Comments on Patient Consent/Data Segmentation

- ***<u>Question 2:</u> How can MU help improve the capacity of EHR infrastructure to record consent, limit the disclosure of this information to those providers and organizations specified on a consent form, manage consent expiration and consent revocation, and communicate the limitations on use and restrictions on re-disclosure to receiving providers?***
  - Create and adopt standards to improve the capacity of EHR infrastructure
  - Create standardized fields for specially protected health information
  - Require all certified EHRs manage patient consent and control re-disclosure

- ***<u>Question 3:</u> Are there existing standards, such as those identified by the Data Segmentation for Privacy Initiative Implementation Guide, that are mature enough to facilitate the exchange of this type of consent information in today's EHRs and HIEs?***
  - Many comments call attention to segmentation-related initiatives that might be leveraged , such as:
    - S&I Framework's Data Segmentation for Privacy Initiative (DS4P WG)
    - HL7 confidentiality and sensitivity code sets
    - SAMHSA/VA pilot
    - eHI developed the "eHealth Initiative Blueprint: Building Consensus for Common Action"

OCPO - Research & Policy Implementation Activities

- Research
  - Privacy and Security Consumer Attitudes Survey
  - mHealth Consumer Attitudes Focus Groups
  - Endpoint Security Device Testing Project
  - Strategic Health IT Advanced Research Projects on Security (SHARPS)
  - ID Proofing/Credentialing
  - Notice of Privacy Practices with OCR
- Policy Implementation
  - Data Segmentation for Privacy Initiative
  - eConsent Trial Project
  - Mobile Devices for Providers
  - Health Care Provider Resources
  - Resilience Planning for HIEs (Disaster Recovery)
  - Technical Assistance

Data Segmentation for Privacy Initiative

- Enable the implementation and management of disclosure policies that:
  - Originate from the patient, the law, or an organization.
  - Operate in an interoperable manner within an electronic health information exchange environment.
  - Enable individually identifiable health information to be appropriately shared.
  - Builds on NCVHS and PCAST recommendations
- Example user stories include:
  - Information related to substance abuse treatment, which is given heightened protection under the law.
- Implementation guides completed; Pilot demos at HIMSS
- For more information: http://wiki.siframework.org/Data+Segmentation

eConsent Project Background & Objectives

In a clinical setting…

- Design, develop, and pilot innovative ways to:
  - Educate patients about their option to make an individual choice (or patient consent) about whether or not their health care provider can share/access their health information through a health information exchange organization (HIE) (*Meaningful Choice*);
  - Assess patients' knowledge gained and their individual satisfaction with the educational material and associated electronic delivery method; and
  - Electronically capture and record a patient's choice.

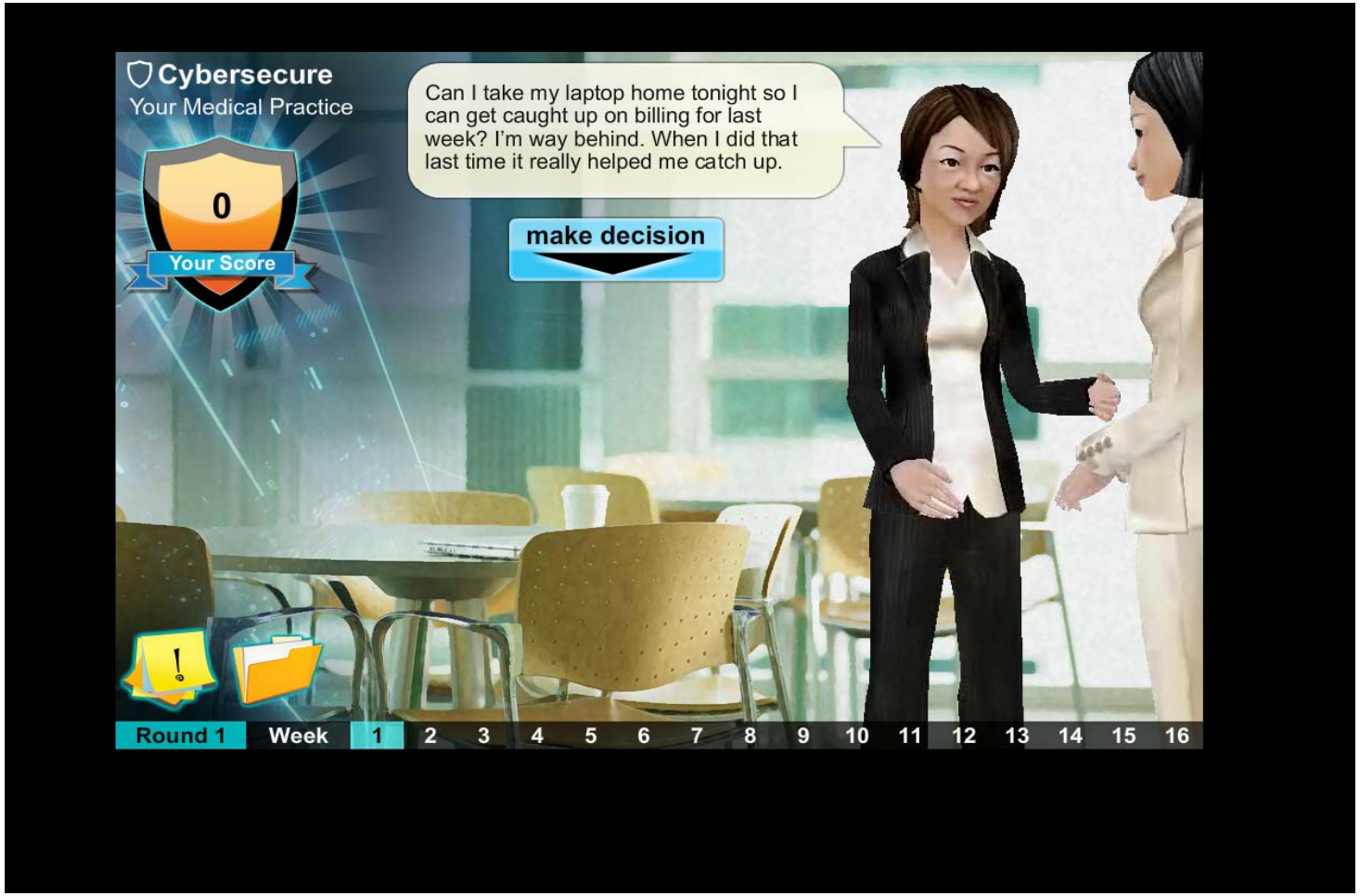
Health IT Policy Committee Individual Choice Recommendations (September 2010) informed project objectives.

Anticipated Project Outputs

- Identification of effective and innovative resources and examples that help ensure:
  - Any choices patients make with respect to sharing their health information are indeed, meaningful.
  - Patients understand the consequences of their choice.
  - Patients better understand their choice regarding whether and when their health care provider can share their health information electronically, including sharing it with a health information exchange organization.
- Project Timeline: October 2011 – March 2013

Security Training Game

Screenshot from game for providers:



Take the Steps to Protect and Secure Health Information when Using a Mobile Device

The resource center HealthIT.gov/mobiledevices was created to help providers and professionals:

Protect and Secure health information when using mobile devices

- In a public space
- On site
- At a remote location

Regardless of whether the mobile device is

- Personally owned, bring your own device (BYOD)
- Provided by an organization

Notice of Privacy Practices with OCR

- Objectives:
  - Use innovative ways to:
    - Identify barriers to consumer understanding of HIPAA Privacy Rule notices of privacy practices for protected health information
    - Propose several alternative formats or approaches to HIPAA Privacy Rule notices of privacy practices (*i.e.*, possible wording, presentation formats, or complete sample privacy notices) that communicate more effectively to consumers while still conforming to regulatory requirements.
  - Explore and evaluate these proposed alternative formats or approaches in simulated situations with consumers to observe their usage of the notices.
- Timing: October 2012 – March 2014. Focus group conducted; Commencement of Design phase.

Privacy and Security Consumer Attitudes Survey

- Objectives:
  - Identify and explore attitudes and preferences of consumers with respect to the privacy and security aspects of EHRs and health information exchange
  - Identify changes in consumer attitudes over time
  - Intent is to survey on at least core questions through 2014
  - Leveraging HINTs survey
- Status:
  - Completed; results being analyzed

mHealth Focus Groups

- mHealth Consumer Attitudes Focus Groups
  - Text messaging, email, Skype and use of apps
  - HHS Text4Health Task Force identified privacy and security of mHealth as critical issue to be explored
    - http://www.hhs.gov/open/initiatives/mhealth/index.html
- Objectives:
  - Identify and explore attitudes and preferences of consumers with respect to mHealth privacy and security
  - Explore potential safeguards
- Status:
  - Completed; report in internal clearance

QUESTIONS