

The Office of the National Coordinator for
Health Information Technology



ONC Privacy and Security Update

August 1, 2012

Joy Pritts, JD
Chief Privacy Officer

Putting the **I** in **HealthIT**
www.HealthIT.gov

State HIE Privacy and Security Program Information Notice



- Issued March 2012
- Gives guidance on expectations for privacy and security frameworks based on Fair Information Practices
- Incorporates HIT Policy Committee recommendations regarding:
 - Informed choice to participate
 - Strong provider authentication
- 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
 - Search “state program information notice”



- National Strategy for Trusted Identities in Cyberspace (NSTIC)
 - Administration initiative
 - One-time ID-proofing
 - Credential accepted by multiple parties
- HIT Policy Committee, P&S Tiger Team Hearing
 - Provider focus, July 11, 2012
 - Patient-focus, later this year



- Final Rule sent to OMB March 24, 2012
- Key provisions
 - Finalizes breach notification rule
 - Extends use and disclosure provisions of HIPAA Privacy Rule and most requirements of HIPAA Security Rule to business associates



- Accountable Care Organizations Final Rule
 - Federal Register, vol. 76 Page 67802 (11/02/11)
- ACOs may be business associates
- Providers in ACO are eligible to receive Medicare claims data generated by other providers
- Individuals may opt out of having certain identifiable information shared



- Final Rule on Availability of Medicare Data for Performance Measurement
 - Federal Register, vol. 76, page 76542 (12/07/11)
- Qualified entities (conduct data analytics)
 - Are not considered business associates of CMS
 - Must have a rigorous data privacy and security program to qualify to receive Medicare data
 - Must sign a stringent data use agreement



- Establishment of Exchanges and Qualified Health Plans Final Rule
 - Federal Register, vol. 77, page 18310 (03/27/12)
- 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

Snapshot of OCPO Research & Internal Initiatives



- Data Segmentation for Privacy Initiative
- eConsent Trial Project
- Mobile Device Portfolio
- Privacy and Security Consumer Attitudes Survey

Data Segmentation for Privacy Initiative Overview

- Underlying Challenge:
 - 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.
- Initiative builds on the PCAST vision and recommendations from the HITSC for the development of metadata tags to be used for exchanging data across organizational structures while maintaining the privacy and security of the information.

Data Segmentation for Privacy Initiative



- Example user stories include:
 - Information related to substance abuse treatment, which is given heightened protection under the law.
- Standards assessment completed
- Pilot selected
- Delayed due to funding
- For more information: <http://wiki.siframework.org/Data+Segmentation>

Completed Use Case available for review at:

<http://wiki.siframework.org/Data+Segmentation+WG+Consensus>

- Includes 6 scenarios that demonstrate need for:
 - Push and pull transactions
 - Protection of substance abuse, HIV, and Sickle-Cell Anemia treatment information (as defined by 42 CFR Part 2 and 38 U.S.C. § 7552)
 - Electronic implementation of HITECH modification of HIPAA that allows patient to withhold information from payers when paying out of pocket for their care

E-Consent Trial: Project Objectives



- HIT Policy Committee Recommendations on Individual Choice
- Design, develop, and pilot innovative ways to:
 - Educate and inform individuals of their option to give individual choice in a clinical setting to share their health information electronically.
 - Ensure that individuals are knowledgeable participants in decisions about sharing their electronic health information in a clinical environment.
 - Electronically obtain and record meaningful choice from individuals in a clinical setting.
- Project Timeline: October 2011 – March 2013



- Mobile health “good practices” project with OCR
 - Roundtable and other information gathering
 - Testing of smart phones, tablets “out of box” security
 - Output: Educational materials in various formats
 - Project Timeline: January 2012 – October 2012



- mHealth Consumer Attitudes Survey
 - 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
 - Timeline: November 2011 – October 2012



- SHARPS
 - Strategic Healthcare IT Advanced Research Projects on Security
 - Implantable medical devices and security
 - Consumer attitudes regarding privacy and remote monitoring devices

Consumer Privacy and Security Perspectives Survey

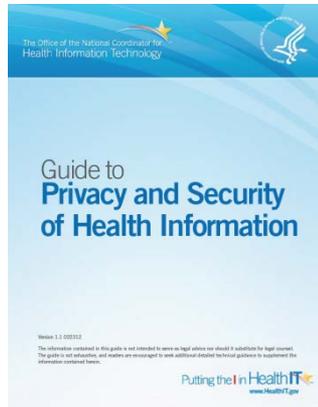


- Objectives:

- 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

Timing: Ready to launch

Helping Providers Integrate Privacy and Security into Their Culture



*OCPO developed this guide with assistance from an ONC cooperative agreement partner, the American Health Information Management Association (AHIMA) Foundation.

We recently released a [Guide to Privacy and Security of Health Information](#),

Designed to help health care practitioners and practice staff better understand the important role privacy and security in the use of EHRs and how to conduct the best practices to safeguard health information

Privacy and security are key components to building the trust required to realize the potential benefits of electronic health information exchange. Protecting the privacy and security of health information must be a primary goal of health care providers and organizations. It's also a vital part of Meaningful Use.

We issued the guide to give providers/organizations with a useful tool to help them integrate privacy and security into their medical practices (including HIPAA and Meaningful Use requirements).

Overall goal of the goal of the guide is to help ensure the privacy and security of health information, including information in electronic health records (EHR) and mobile devices.

Instructional guide designed to help healthcare practitioners, staff, and other professionals better understand the important role privacy and security play in the use of electronic health records (EHRs) and Meaningful Use.

- Designed to help health care practitioners and practice staff understand the importance of privacy and security of health information at various implementation stages
- Developed with assistance from the American Health Information Management Association (AHIMA) Foundation, with input from OCR and OGC

Available at

<http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf>

Training Materials: Series of Security Video Games Due for Release Summer of 2012



Cybersecure
Your Medical Practice

0
Your Score

Can I take my laptop home tonight so I can get caught up on billing for last week? I'm way behind. When I did that last time it really helped me catch up.

make decision

Round 1 Week 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

We are working on other activities to assist providers...



Questions?