



The Office of the National Coordinator for
Health Information Technology



ONC Privacy & Security Policy Update

**NCVHS Full Committee
Meeting
June 19, 2013**

Kathryn Marchesini, JD



Office of the Chief Privacy Officer

The Office of the National Coordinator for
Health Information Technology

- Issue before the HITPC Privacy & Security Tiger Team
- Update on a subset of OCPO projects
 - Consumer Privacy & Security Survey
 - Data Segmentation for Privacy (DS4P)
 - Privacy and Security Educational and Training Materials

Virtual Hearing on Non-Targeted Query



- HITPC's Privacy & Security Tiger Team's Public Hearing on June 24, 2013, 1 – 4 EDT
- An effort to
 - Gain an understanding of what type of policies are deployed to ensure that a “non-targeted query” for a patient record is appropriate, legal, and authorized
 - Learn about the thought processes behind the development of any such policies

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
 - Survey on at least core questions through 2014
 - Leverage HINTs survey
- Status:
 - Completed; results being analyzed

Data Segmentation for Privacy Initiative (DS4P)



- Standards and Interoperability Initiative
- Strong Community Participation
 - 306 Participating Individuals
 - 100 Committed Members
 - 94 Participating Organizations
- For more information:
<http://wiki.siframework.org/Data+Segmentation>

DS4P Pilot Status



Pilot Name	Development Status	Data Types/ Policies	Status	Use Case Scenarios	Scalability
VA/ SAMHSA	Testing Complete	Title 38 Section 7332 -Sickle cell anemia -HIV related information -Substance abuse information	As of June 2013, pilot has tested all applicable parts of the DS4P Implementation Guide	Direct and Exchange, incl. Break Glass	<ul style="list-style-type: none"> • Capabilities being integrated into iEHR and eHealth Exchange • Intended to be offered as enterprise access control service
Software & Technology Vendors Association SATVA	Requirements Development /Technical Testing	42 CFR Part 2, NY HIV (planned)	Production in 2013	Direct and Exchange incl. Break Glass	<ul style="list-style-type: none"> • Anasazi Exchange and HEALTHeLink agreed to pilot to Anasazi providers
NETSMART	Testing with Tampa 2-1-1 system	42 CFR Part 2 HIV Status (Public Health)	Pilot evaluation results Sep/Oct 2013	Direct and Exchange	<ul style="list-style-type: none"> • Plans to work with Illinois HIE, Kansas Health Network and Tampa Bay Network to pilot
JERICH0/ University of Texas	Requirements Development (Early Stages)	42 CFR Part 2	Dec 2013	HIE/Exchange Scenarios	<ul style="list-style-type: none"> • A provider and government agency are considering participation
Greater New Orleans HIE GNOHIE	Completing Sprints, Developing Test Cases	42 CFR Part 2	Pilot evaluation results Sep/Oct 2013	HIE/Exchange Scenarios	<ul style="list-style-type: none"> • Records for approx 215K patients from 10 organizations and 21 clinics



- Security 101 Awareness Video Series
 - Introduction to fundamentals of information security topics for small and medium size providers
 - Development coordination with HHS Office for Civil Rights (OCR)
 - Anticipated release date on healthIT.gov in Fall 2013

Security Training Game – Part II

www.healthIT.gov



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

! Folder

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

Mobile Device Privacy & Security Resource Center – Phase II Materials

Materials available on HealthIT.gov/mobiledevices include:

- Fact sheets
- Posters
- Brochures
- Postcard
- Educational videos



Mobile Devices: Know the RISKS. Take the STEPS.
PROTECT & SECURE Health Information.
Find out more at HealthIT.gov/mobiledevices.

10 tips to protect and secure health information when using a mobile device.

- 1 Use a password or other user authentication
- 2 Install and enable encryption
- 3 Install and activate remote wiping or remote disabling
- 4 Do not install or use file sharing applications
- 5 Install and enable a firewall
- 6 Install security software and keep it up to date
- 7 Research mobile applications before downloading
- 8 Always keep your device in your possession
- 9 Use adequate security to send or receive health information over public Wi-Fi networks
- 10 Delete all stored health information before discarding the mobile device



Managing Mobile Devices in Your Health Care Organization

Health care providers and professionals are using mobile devices in their work. Covered entities must comply with HIPAA privacy and security rules to protect and secure health information, even when using mobile devices. As a leader within your organization, you are responsible for developing and implementing mobile device procedures and policies that will protect the health information patients entrust to you.

Here are the steps your organization can take to help manage mobile devices in your health care setting.

1. Evaluate whether mobile devices will be used to access, transmit, to receive, or store patients' health information or be used as part of your organization's internal network or systems, such as an electronic health record system. Understand the risks to your organization before you decide to allow the use of mobile devices.
2. Consider the risks when using mobile devices to transmit the health information your organization holds. Conduct a risk analysis to identify threats and vulnerabilities. If you are a solo provider, you may conduct the risk analysis yourself. If you work for a large provider, the organization may conduct it.
3. Identify a mobile device risk management strategy, including policy and security safeguards. A risk management strategy will help your organization identify and implement mobile device safeguards to reduce risks identified in the risk analysis, including an evaluation of regular maintenance of the mobile device safeguards you put in place.
4. Develop, document, and implement your organization's mobile device policies and procedures to safeguard health information. Some topics to consider when developing mobile device policies and procedures are:
 - Mobile device management
 - Using your own device
 - Restrictions on mobile device use
 - Security or configuration settings for mobile devicesIdentify mobile device privacy and security weaknesses or ongoing training for providers and professionals.

Know the RISKS. Take the STEPS.
CARE Health Information.
HealthIT.gov/mobiledevices



Mobile Devices: Know the RISKS. Take the STEPS.
PROTECT and SECURE Health Information.

Is your information protected? Mobile devices are easily lost or stolen. Avoid losing or disclosing patients' health information. Keep your mobile device with you. Learn more at HealthIT.gov/mobiledevices.



Be a team player.
Understand and follow your organization's mobile device policy and procedures. *It's your responsibility.*
Visit HealthIT.gov/mobiledevices



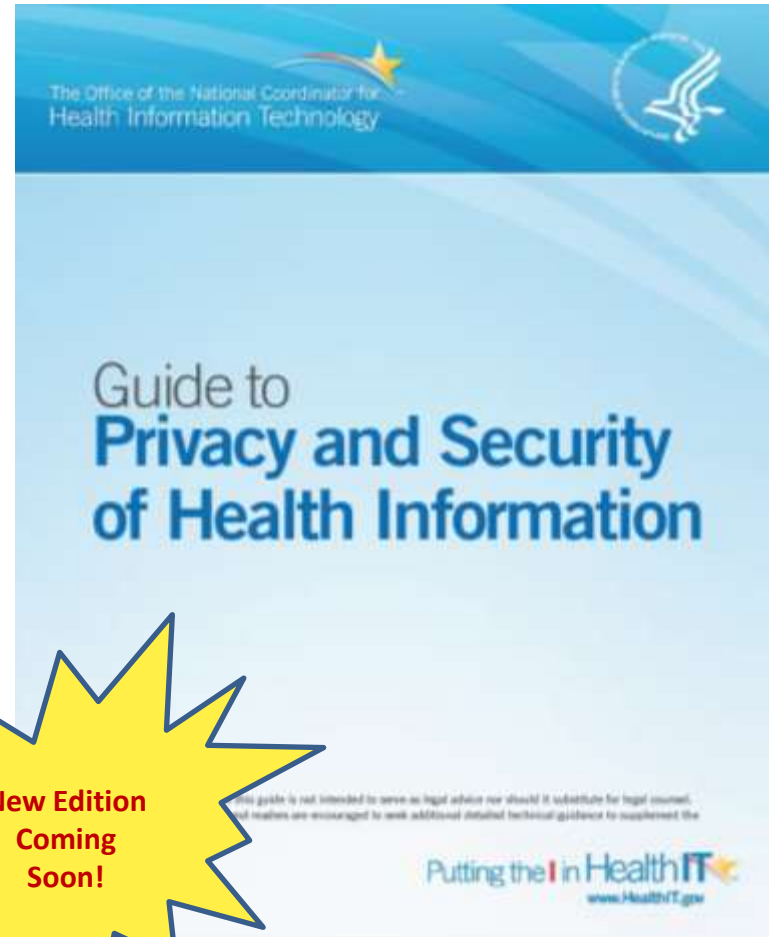
Mobile Devices: Know the RISKS. Take the STEPS.
PROTECT and SECURE Health Information.



Helping Providers Integrate Privacy and Security into Their Culture



- Designed to help health care practitioners and practice staff understand 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 HHS OCR and OGC
- Updating to reflect HITECH & MU updates



**New Edition
Coming
Soon!**

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



Questions?