The Office of the National Coordinator for
Health Information Technology

ONC
Privacy and Security Update

May 7, 2013

Joy Pritts, JD
Chief Privacy Officer

HITECH Modifications to HIPAA

- OCR published Final Rule January 25, 2013 2013
- Compliance date September 23, 2013

HITECH Modifications to HIPAA

- Some 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
  - Clarifies patient right to access electronic health information
  - Patient right to restrict providers disclosing health information to plans when paying out of pocket

Executive Order 13636—
Improving Critical Infrastructure Cybersecurity

- Published February 19, 2013
- Health and public health care considered to be a critical infrastructure sector (since 2003)
- http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

Executive Order 13636—
Improving Critical Infrastructure Cybersecurity

- Increase government sharing cybersecurity information with private sector critical infrastructure and state and local governments
- NIST to lead development of a framework to reduce cyber risks

Executive Order 13636—
Improving Critical Infrastructure Cybersecurity

- Identifying critical infrastructure at greatest risk—cybersecurity incident could reasonably result in *catastrophic* regional or national effects on public health or safety, economic security, or national security
- A very high bar

NSTIC: Health Related Pilot Overview

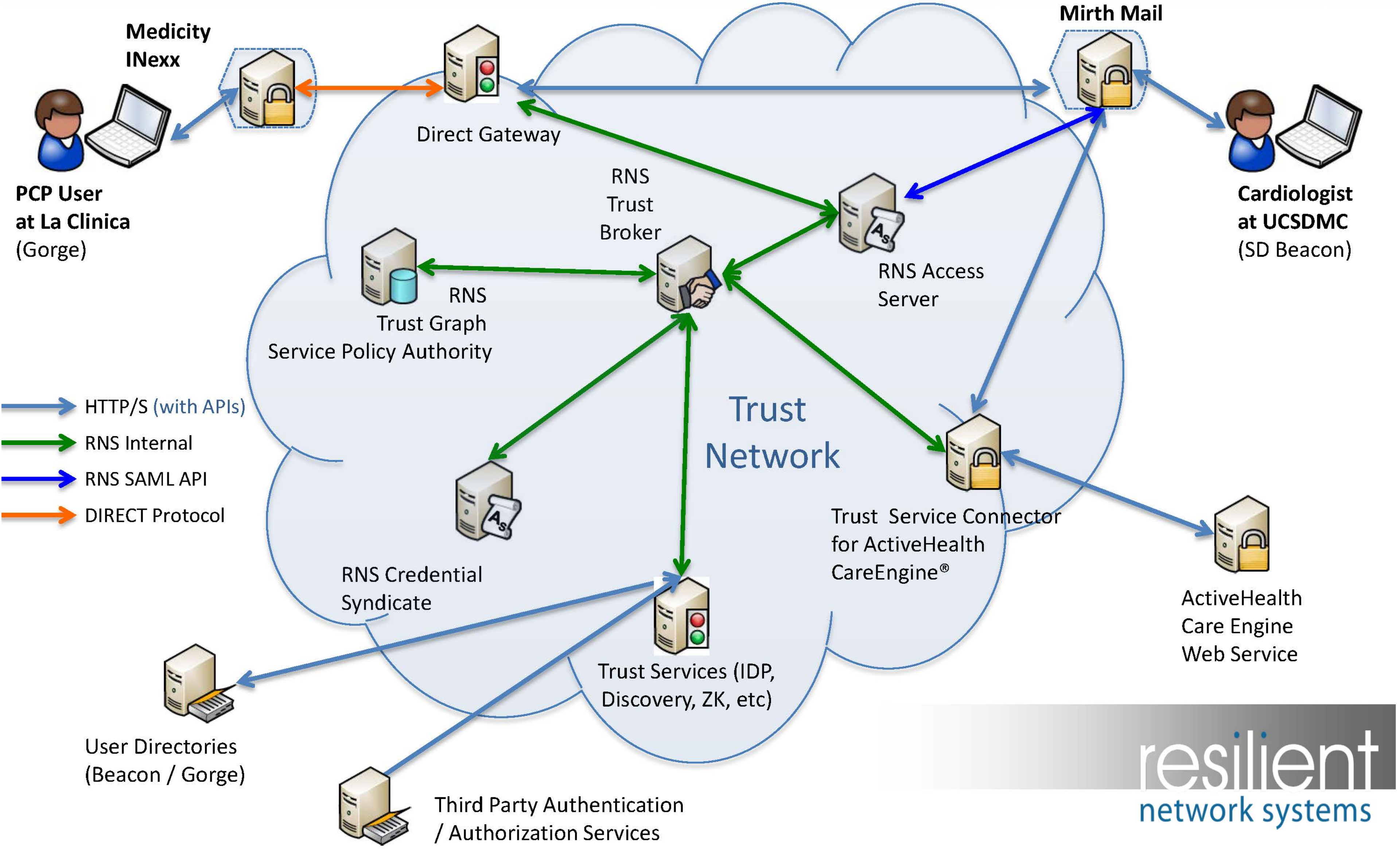
Resilient Network Systems, in partnership with the American College of Cardiology (ACC), The American Medical Association (AMA), LexisNexis, NaviNet, ActiveHealth Management, the San Diego Beacon eHealth Community, Gorge Health Connect, the Kantara Initiative, and the National eHealth Collaborative (NeHC) will implement a Trust Network infrastructure to enable convenient multi-factor, on-demand identity proofing and authentication of patients, physicians and staff on a national scale.

The pilot’s use cases will facilitate patient-centered coordination of care among a select group of primary care physicians and cardiologists by enhancing existing automated systems for secure, HIPAA-compliant access to electronic referral (eReferral) and Transfer of Care messaging and an advanced clinical decision support service.

NSTIC Pilot Participants

- **San Diego Beacon eHealth Community**
  - Select subset of physicians as pilot sites
  - Interface with their Mirth Mail messaging system with Direct HISP
  - Access their Axolotl HIE platform
- **Gorge Health Connect**
  - Select subset of physicians as pilot sites
  - Interface with their Medicity iNexx eReferral system with Direct HISP
  - Access their Medicity HIE platform
- **Policy Authority Service**
  - Neutral policy authority service on Trust Network will mitigate liability by ensuring alignment of policies and services to comply with relevant regulations and best practices.
- **National eHealth Collaborative (NeHC)**
  - Publish neutral policy authority service on Trust Network to mitigate liability by ensuring alignment of policies and services to comply with relevant healthcare regulations
  - Coordinate HIE stakeholders to advise on policy and technology requirements for pilot phases, and plans for transition to production and commercialization

PCC Pilot Overview



resilient
network systems

Current Status

- The Direct gateway has been prototyped & preliminarily tested.
- The ActiveHealth integration is being prototyped now.
- Agreements in place for use of directories, attribute providers & the eReferral tools.

Snapshot of OCPO Research & Internal Initiatives

- Data Segmentation for Privacy Initiative
- Mobile Device Security Resources
- Privacy and Security Educational and Training Materials

Data Segmentation for Privacy: HITECH Mandate

Public Health Service Act Sec. 3002 (2)

The HIT Policy Committee shall make recommendations for at least the following areas: ''(i) Technologies that protect the privacy of health information and promote security in a qualified electronic health record, including for the segmentation and protection from disclosure of specific and sensitive individually identifiable health information with the goal of minimizing the reluctance of patients to seek care (or disclose information about a condition) because of privacy concerns, in accordance with applicable law."

HITPC Prior Proceedings

- Tiger Team hearing on technology in Summer 2010
- Recommendations September 2010
  - Technology is promising but in early stages
  - Need to further experience and stimulate innovation for granular consent
  - ONC should make it a priority to further explore
  - Find evidence (such as through pilots) for models that have been implemented successfully
- ONC gave HITPC last update Fall 2012

Data Segmentation for Privacy Initiative

- Standards and Interoperability Initiative
- Strong Community Participation
  - – 306 Participating Individuals
  - – 100 Committed Members
  - – 94 participating Organizations

Initiative Accomplishments

- Data Segmentation for Privacy Use Case document. Uses include electronically implementing existing laws including:
  - 42 CFR Part 2: Federal Confidentiality of Alcohol and Drug Abuse Patient Records regulations protect specific health information from exchange without patient consent. Recipient may not re-disclose without patient consent.
  - Title 38, Section 7332, USC : Laws protecting certain types of health data coming from covered Department of Veterans Affairs facilities and programs. Types of data include sickle cell anemia, HIV, and substance abuse information.

Initiative Accomplishments

- Implementation Guide describing recommended standards for privacy metadata, organized by transport mechanism:
  - **SOAP**: Provides support for NwHIN / eHealth Exchange.
  - **SMTP**: Provides support for DIRECT (
  - **REST**: HL7 hData Record Format or IHE Mobile Access to Health Documents (MHD) Profile.
- Analysis of HITSC recommendations for privacy metadata supporting the PCAST vision for tagged data elements.
- Executive Summary Document (Community Draft)
- DS4P Implementation GuideTest Procedures

Technical Approach

Layered Approach for Privacy Metadata

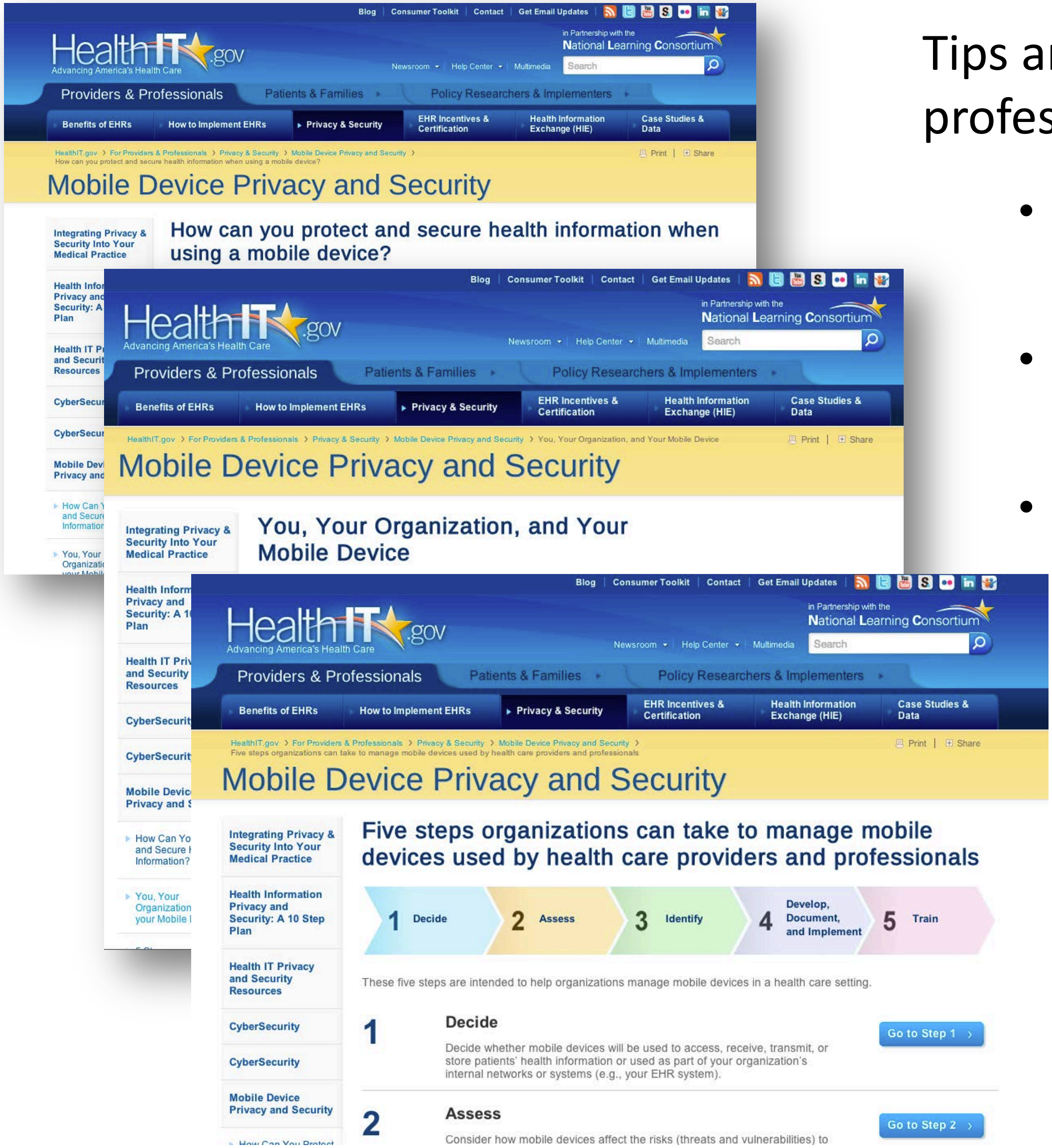
- “Russian doll” concept of applying metadata with decreasing specificity as layers are added to the clinical data.

- Privacy metadata uses standards to convey:
  - Confidentiality of data in clinical payload
  - Obligations of receiving system
  - Allowed purpose of use

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 May 2013 pilot has tested all applicable parts of the DS4P IG	Direct and Exchange, incl. Break Glass	• 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	• 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	•Plans to work with Illinois HIE, Kansas Health Network and Tampa Bay Network to pilot
JERICHO/ University of Texas	Requirements Development (Early Stages)	42 CFR Part 2	Dec 2013	HIE/Exchange Scenarios	• 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	• Records for approx 215K patients from 10 organizations and 21 clinics

Mobile Device Security Resource Center for Providers and Professionals


Blog | Consumer Toolkit | Contact | Get Email Updates
HealthIT.gov
Advancing America's Health Care
in Partnership with the National Learning Consortium
Newsroom | Help Center | Multimedia | Search
Providers & Professionals | Patients & Families | Policy Researchers & Implementers
Benefits of EHRs | How to Implement EHRs | Privacy & Security | EHR Incentives & Certification | Health Information Exchange (HIE) | Case Studies & Data
Print | Share

HealthIT.gov › For Providers & Professionals › Privacy & Security › Mobile Device Privacy and Security › How can you protect and secure health information when using a mobile device?

Mobile Device Privacy and Security

How can you protect and secure health information when using a mobile device?

HealthIT.gov › For Providers & Professionals › Privacy & Security › Mobile Device Privacy and Security › You, Your Organization, and Your Mobile Device

Mobile Device Privacy and Security

You, Your Organization, and Your Mobile Device

HealthIT.gov › For Providers & Professionals › Privacy & Security › Mobile Device Privacy and Security › Five steps organizations can take to manage mobile devices used by health care providers and professionals

Mobile Device Privacy and Security

Integrating Privacy & Security Into Your Medical Practice
Health Information Privacy and Security: A 10 Step Plan
Health IT Privacy and Security Resources
CyberSecurity
CyberSecurity
Mobile Device Privacy and Security
How Can You Protect
You, Your Organization and your Mobile Device

Five steps organizations can take to manage mobile devices used by health care providers and professionals

These five steps are intended to help organizations manage mobile devices in a health care setting.

1 **Decide**

Decide whether mobile devices will be used to access, receive, transmit, or store patients' health information or used as part of your organization's internal networks or systems (e.g., your EHR system).

2 **Assess**

Consider how mobile devices affect the risks (threats and vulnerabilities) to

Tips and information providers and professionals can use to:

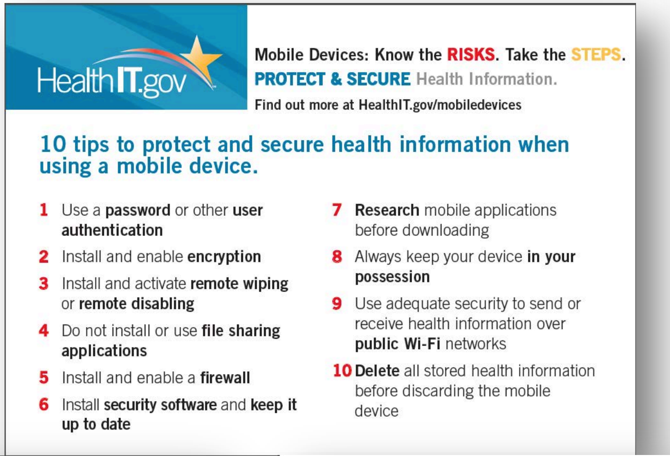
- Protect and secure health information when using a mobile device
- Understand their organization's mobile device policies and procedures
- Five steps organizations can take to manage mobile devices

Materials Available Online

HealthIT.gov

Materials available for download on HealthIT.gov/mobiledevices include:

- **Fact sheets**
- **Posters**
- **Brochures**
- **Postcard**

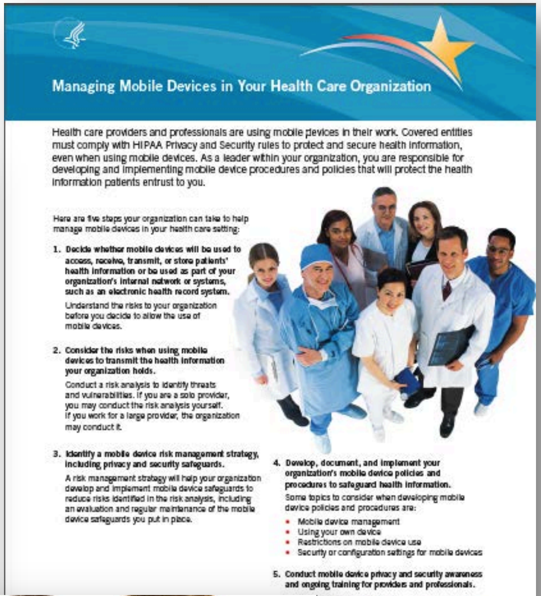


HealthIT.gov

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 pevices 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 five steps your organization can take to help manage mobile devices in your health care setting:

1. **Decide whether mobile devices will be used to access, receive, transmit, 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 privacy and security safeguards.**

   A risk management strategy will help your organization develop and implement mobile device safeguards to reduce risks identified in the risk analysis, including an evaluation and regular maintenance of the mobile device safeguards you put in place.

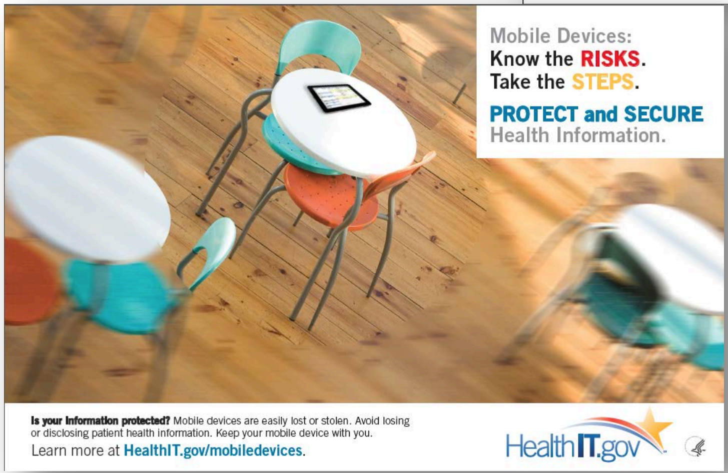
4. **Develop, document, and implement your organization's mobile device policies and procedures to safeguard health information.**

   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 devices

5. **Conduct mobile device privacy and security awareness and ongoing training for providers and professionals.**

w the **RISKS**. Take the **STEPS**.
E Health Information.
T.gov/mobiledevices

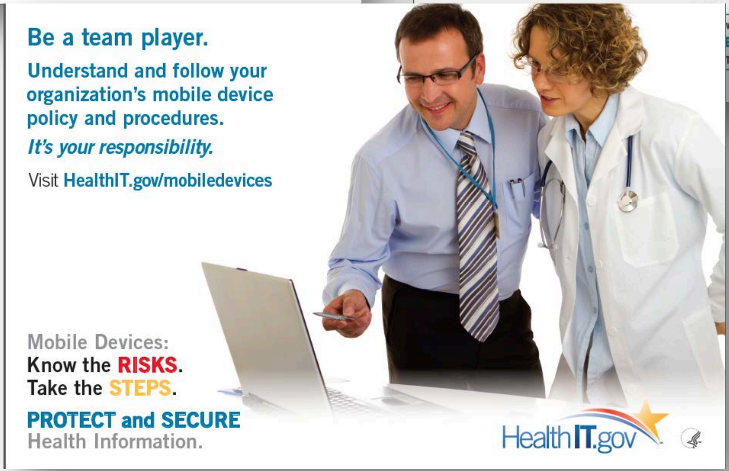


Mobile Devices:
Know the **RISKS**.
Take the **STEPS**.
PROTECT and SECURE
Health Information.

Is your Information protected? Mobile devices are easily lost or stolen. Avoid losing or disclosing patient health information. Keep your mobile device with you.

Learn more at **HealthIT.gov/mobiledevices**.

HealthIT.gov



Be a team player.

Understand and follow your organization's mobile device policy and procedures.

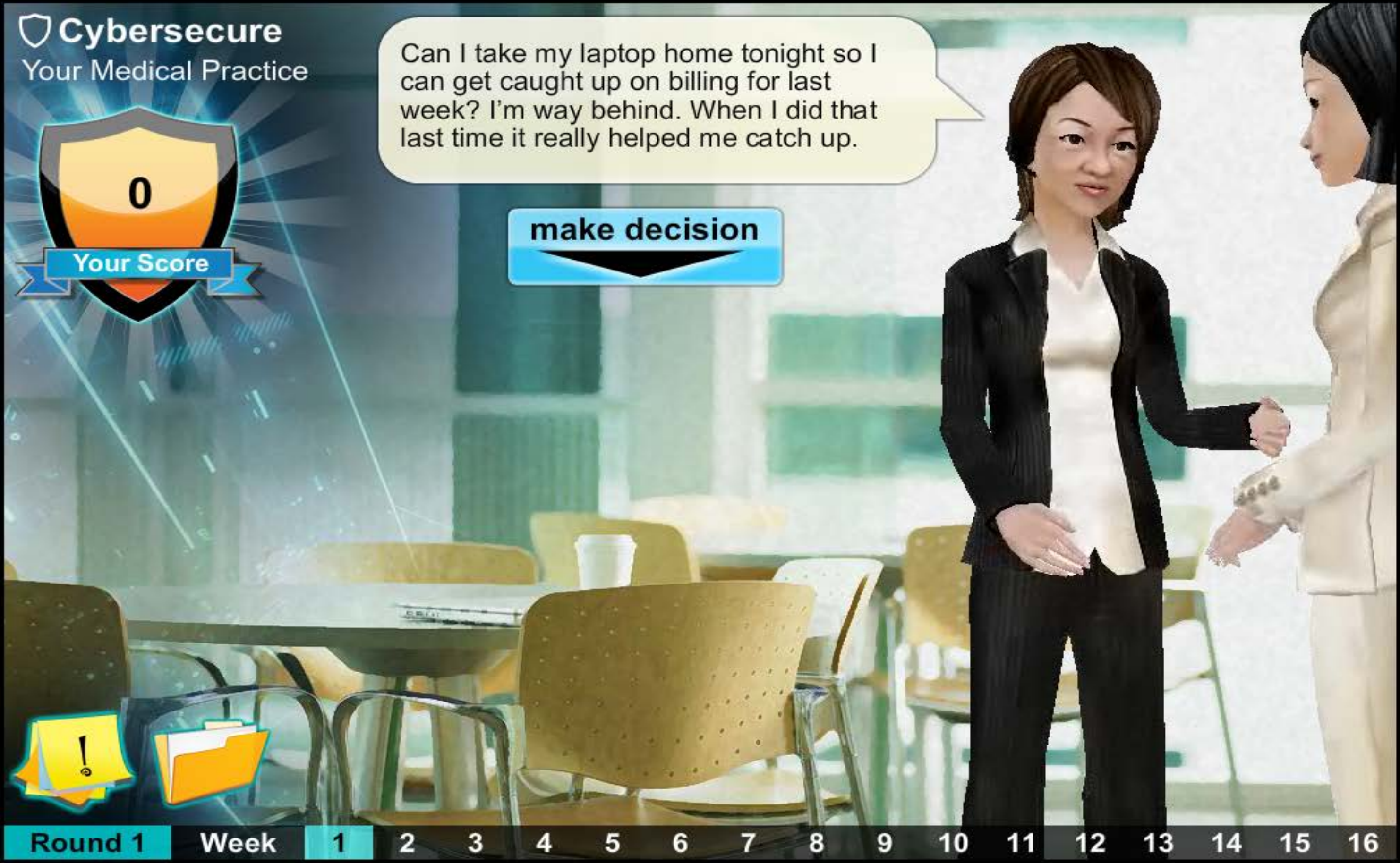
It's your responsibility.

Visit **HealthIT.gov/mobiledevices**

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

HealthIT.gov

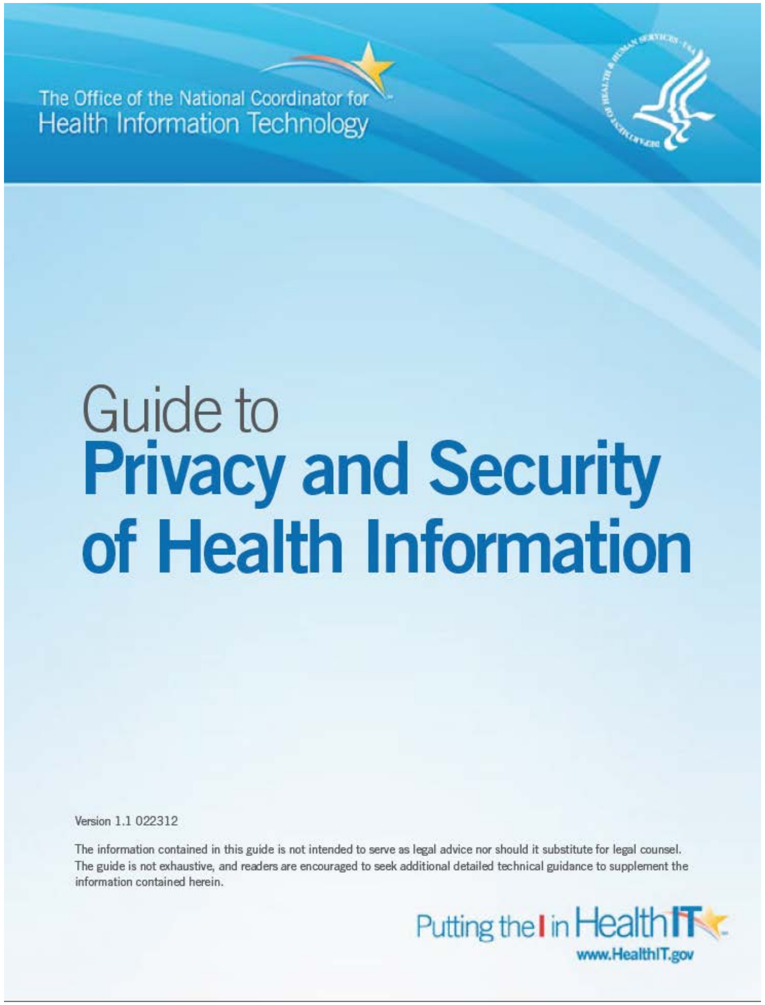
Training Materials: Security Video Game Released



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.

Helping Providers Integrate Privacy and Security into Their Culture

- 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
- Being updated to reflect HITECH changes



The Office of the National Coordinator for
Health Information Technology

Guide to
Privacy and Security of Health Information

Version 1.1 022312

The information contained in this guide is not intended to serve as legal advice nor should it substitute for legal counsel. The guide is not exhaustive, and readers are encouraged to seek additional detailed technical guidance to supplement the information contained herein.

Putting the I in Health IT
www.HealthIT.gov

The End