The Office of the National Coordinator for Health Information Technology

# Overview: Office of the Chief Privacy Officer Security-Related Initiatives

June 6, 2012

Joy Pritts, JD
Chief Privacy Officer

Putting the I in Health IT
www.HealthIT.gov

# OCPO Overview

- Chief Privacy Officer position created in HITECH Act
- OCPO’s responsibilities include:
  - Advise the National Coordinator on privacy, security, and data stewardship of electronic health information
  - Coordinate with other Federal agencies, State and regional efforts, and foreign countries with regard to the privacy, security, and data stewardship of electronic individually identifiable health information

# OCPO Responsibilities: Privacy and Security

- Policy development, coordination and outreach across HHS, federal government, states and internationally
- Programmatic support
- Research

# Federal Health IT Task Force

- Cross agency task force led by OMB and ONC
- Cybersecurity Workgroup
  - Recommended:  investigate means of making security as easy as possible for the provider using health IT

# Security Policy in Some Key Health Related Regulations Other than HIPAA

# Security in Medicare Medicaid EHR Incentives Program

MU Stage 1 requires eligible providers and hospitals to

- Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.
- Certification criteria E H R must be capable of
  - Automatic log-off
  - Encrypting data in transit in accordance with Annex A Federal Information Processing Standards (FIPS) Publication 140-2

# Security in Medicare Medicaid EHR Incentives Program

MU Stage 2 proposed security

- Highlights need to assess the reasonable and appropriateness of encrypting electronic protected health information at rest
- Use secure electronic messaging to communicate with patients (eligible providers)
    - Email
    - Patient portals
    - PHRs

# Security in Medicare Medicaid EHR Incentives Program

MU Stage 2 Certification Criteria

If . .

– E H R technology manages the health information on an end user device; and

– eHI remains stored on device after use of E H R has stopped **then**

– EHI must be encrypted by default (and disabled by a limited set of identified users)

# Patient Protection and Affordable Care Act (ACA)

- Final Rule on Availability of Medicare Data for Performance Measurement
  - Federal Register, vol. 76, page 76542 (!2/07/11)

- 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

# ACA Health Insurance Exchange Rule

- 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

# ONC Programmatic Support

# Regional Extension Centers

- 62 Regional Extension Centers
  - Working with 132,000 primary care providers
  - 70% of small practice providers in rural
  - 75% of federally funded health centers
- Support health care providers to help them adopt and become meaningful users of EHRs

# Some Recent Security Related Projects

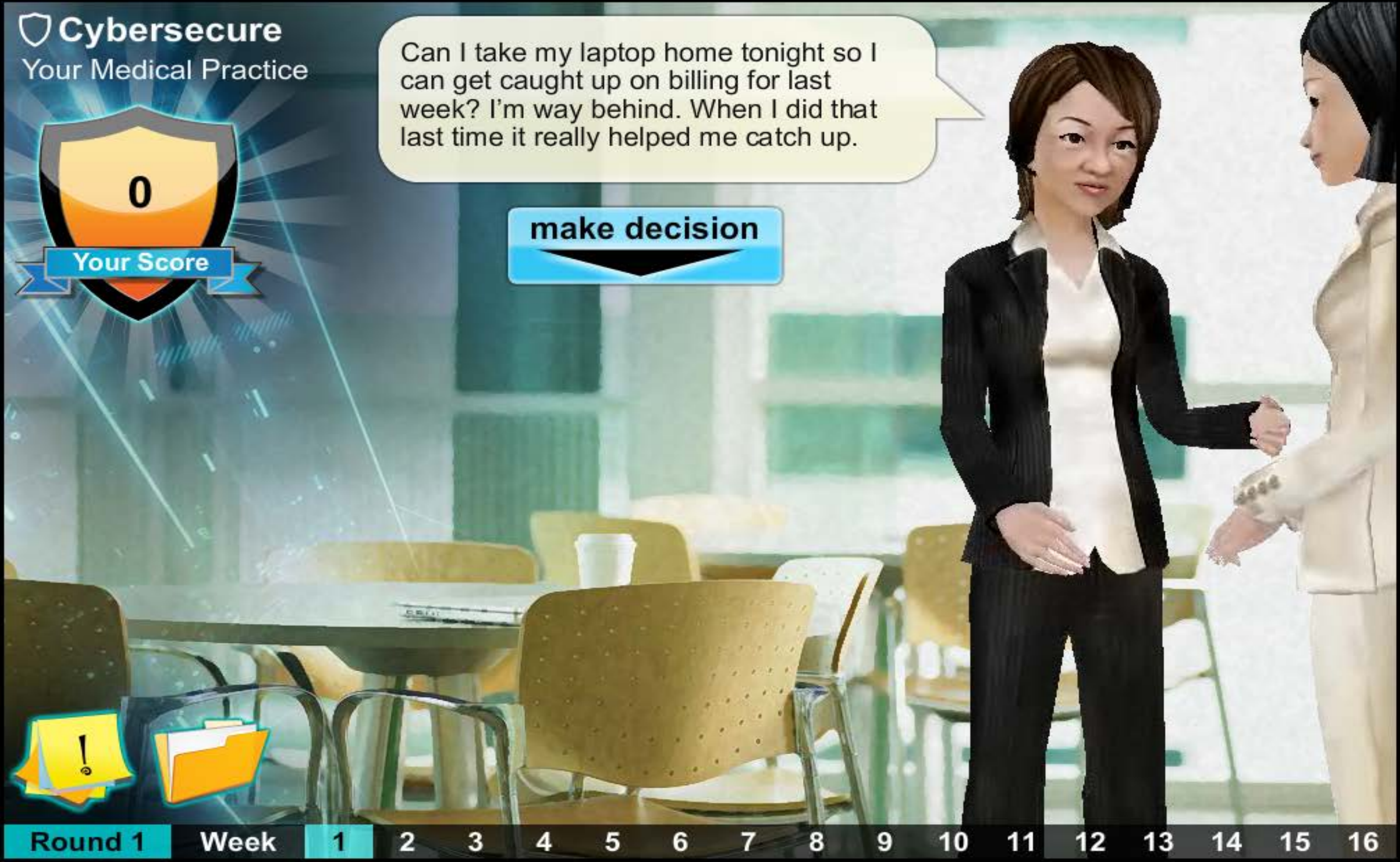
- Data segmentation initiative
- Security training videos
- Mobile devices

# Data Segmentation Initiative

- Standards and Interoperability Framework
- Assessing proposed metadata tag standards for privacy
  - Include some which facilitate access control
- Example user stories include:
  - Information related to substance abuse treatment, which is given heightened protection under the law.

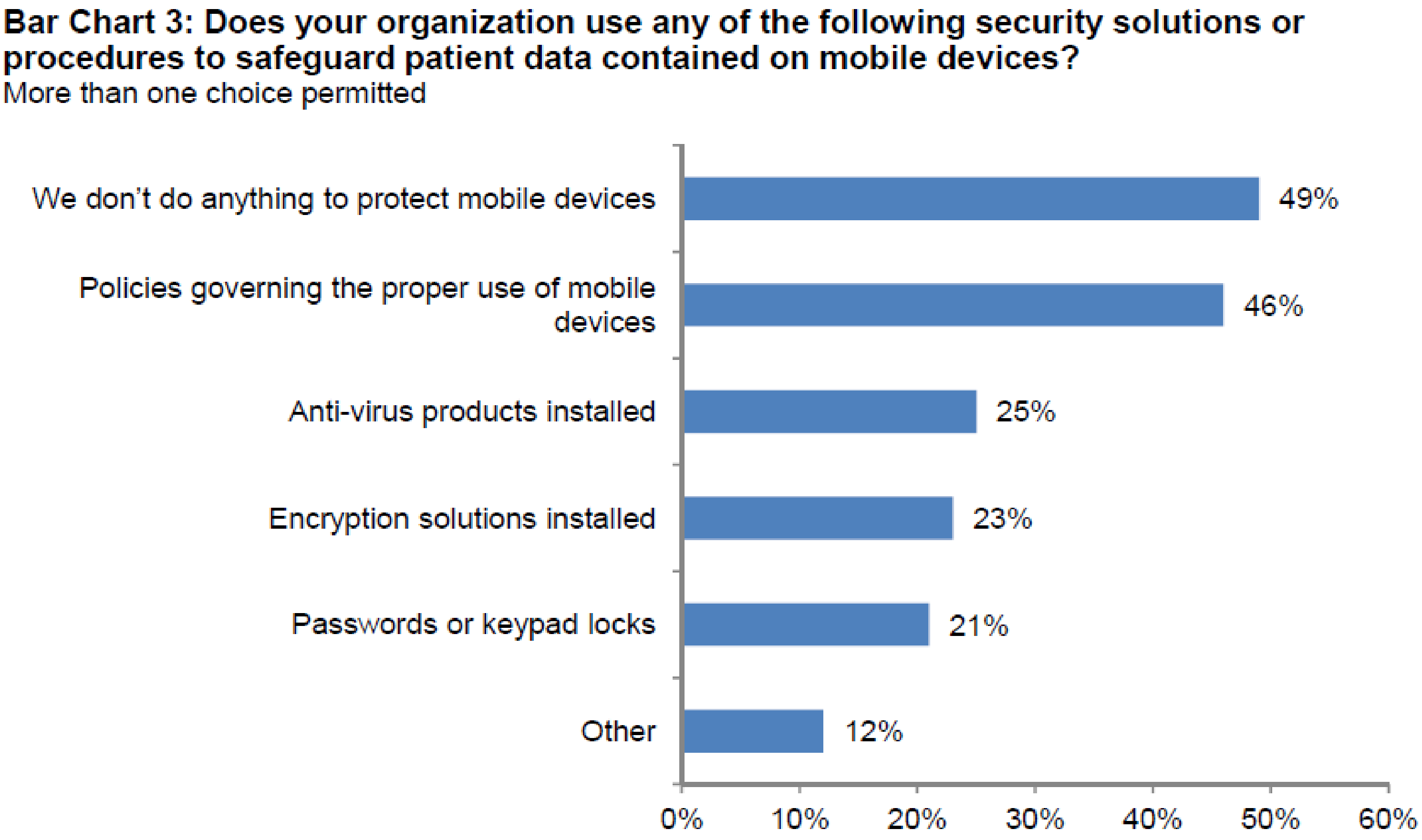
http://wiki.siframework.org/Data+Segmentation+for+Privacy

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



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.

# Mobile Devices



- Ponemon Institute, 2011

# Mobile Device Projects

- Mobile device good practices videos and materials
  - Mobile Device Roundtable
  - Collected public comments
  - Research project on security configurations of mobile devices

# HITEST Lab Devices

## Smartphone devices:

| Device | Operating System | Version |
|---|---|---|
| Apple iPhone 4 | iOS | 4.3.5 & 5.0.1 |
| HTC Vivid | Android 2.3.4 | HTC Sense 3.0 |
| Blackberry Curve | OS 6.0 Bundle 2949 | 6.0.0.668 |
| HTC T9295 Windows Phone | Windows Phone 7.5 OS | 7.10.7720.68 |

# HITEST Lab Devices

## Tablet devices:

| Device | Operating System | Version |
|---|---|---|
| iPad 2 | iOS | 4.3.5 & 5.0.1 |
| Motorola XOOM | Android Honeycomb | 3.2.1 |
| Viewsonic Viewpad | Microsoft OS | Windows 7 Professional |
| Viewsonic Viewpad | Android 2.2 | 1.4 |
| Blackberry Playbook | QNX Software | 1.0.8.6067 |
| HP Touchpad | HP webOS | 3.0.5 |
| Samsung Galaxy Tab | Android OS | 2.2 |

# Configuration is Key

- LMI conducted tests
- Tests showed the level of security “out of the box” and
- Security can be improved with additional configuring on device
- Full briefing on their findings in the break out session  “ONC Mobile Device Project” later today

# Closing Thoughts

We *all* have a role to play in keeping health information private and secure.

- Government should establish P/S policies that are appropriate, affordable and workable
- Vendors should create easy-to-use P/S features and communicate importance
- Providers and staff should understand their role in protecting patient privacy
- Patients should understand their rights and basic means of securing  their PHI

# We Are All in This Together

# Conclusion

**Questions?**