



The Office of the National Coordinator for
Health Information Technology



Creating a Culture Where Privacy and Security Are Understood and Valued

September 20, 2012

Change Management



The screenshot shows the azcentral.com website with a black header bar containing the logo and navigation links for All azcentral.com, Articles, Calendar, and Business. Below the header is a search bar labeled "NEW SEARCH: Find articles, photos, video". The main menu includes News, Sports, Money, Things To Do, Politics, Travel, Weather, Pets, Food & Home, and a Today's Deal section. A sub-menu for Phoenix Jobs, Phoenix Home Sales, Phoenix Home Values, Phoenix Homes For Sale, and Phoenix Apartments is also visible. The main content area features a section titled "ARIZONA BUSINESS & MONEY" with an article about cardiologists being fined \$100,000 for Internet privacy violations.

Cardiologists fined \$100,000 for Internet privacy violations

by Ken Altucker - Apr. 17, 2012 01:37 PM
The Republic |azcentral.com

The federal government has fined a Phoenix and Prescott cardiac surgeon medical practice \$100,000 for posting patients' clinical and

The screenshot shows a Forbes article from April 19, 2012, at 11:44 AM, with 868 views. The article is titled "Arizona Cardiac Surgeons Pay \$100,000 To Settle HIPAA Violations". It discusses how an Arizona cardiac surgery group agreed to pay \$100,000 to resolve an investigation into potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The article notes that the surgical group did not offer an admission of liability but did agree to implement a corrective action plan in addition to the payment. It also mentions that the investigation was conducted by the Health and Human Services Office for Civil Rights (OCR).

An Arizone cardiac surgery group has agreed to pay \$100,000 to resolve an investigation into potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). In the agreement the surgical group did not offer an admission of liability but did agree to implement a corrective action plan in addition to the payment.

According to the Health and Human Services Office for Civil Rights (OCR), the investigation of Phoenix Cardiac Surgery, PC, which is owned by two

The screenshot shows an InformationWeek Healthcare article titled "Online Calendar Mistakes Cost Doctors Group \$100,000". The article discusses how HHS penalized Phoenix Cardiac Surgery for violating HIPAA privacy regulations, including making patient appointments publicly available on the Internet. It notes that Phoenix Cardiac Surgery has agreed to pay the U.S. Department of Health and Human Services (HHS) \$100,000 for posting patient information on the Internet without adhering to federal privacy and security safeguards for personal health information. The settlement follows an investigation by the HHS Office for Civil Rights (OCR) into potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy and security rules.

The OCR investigation was sparked by a report that Phoenix Cardiac Surgery was posting clinical and surgical appointments for its patients on an Internet-based calendar that

More Healthcare Insights

Webcasts

- Learn how Kettering Health Network maximized clinician patient time by virtualizing clinician access to data

Health Data Security: Tips And Tools

(click image for larger view and for



Case Study: Phoenix Cardiac Surgery



Initial Complaint:

- July 2007 to February 2009, Practice posted over 1,000 separate entries of ePHI on a **publicly accessible, Internet-based calendar**
- September 2005 until November 2009, Practice daily transmitted ePHI from an **Internet-based email account to workforce members' personal Internet-based email accounts**

Findings



- **Failure** to implement adequate **policies and procedures** to appropriately safeguard patient information
- **Failure** to document any **employee training** on its policies and procedures on the Privacy and Security Rules
- **Failure** to identify a **security official** and **conduct a risk analysis**
- **Failure** to obtain **business associate agreements** with Internet-based email and calendar services that included storage of and access to its PHI

Privacy and Security: A Shared Responsibility



- Government should establish and enforce P/S regulations that are affordable and workable
 - Vendors should create easy-to-use P/S features and communicate importance
- Providers should understand P/S requirements, establish and promote P/S policies & practices, train and monitor staff, mitigate risk
- Patients should understand their rights and basic means of securing their PHI

Developing a Privacy and Security Culture



Challenges:

- Providers and staff may have little understanding of new technology and privacy and security issues
- Providers and staff are reticent about asking questions or for assistance
- Adopting new software and workflow in the fast-moving healthcare culture is difficult
- Vendors may assume that providers and staff understand privacy and don't always offer adequate training

Leadership Sets the Tone



Protecting
privacy and
securing health
information is
good for our
patients and for
our business

Privacy and Security Metrics are Included in Employee Performance Plans/Evaluations



- Log off routinely when you leave the computer.
- Locks the door when leaving for the day.
- Has completed all necessary training.

Everyone Feels Comfortable Asking Questions and Making Suggestions



How do I make sure that the E H R they are trying to sell me can encrypt information?

Can I use my own smart phone to access medical records?



Some Other Strategies

- Use technology that has privacy and security built into the technology
- Privacy and security are considered as part of physical environment, patient care, and all communications.
- Have privacy and security checkups and communicate results to all.
- Training, is regular and updated and an essential part of the overall strategic plan.



The Office of the National Coordinator for
Health Information Technology



ONC Projects and Tools

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

Snapshot of OCPO Research & Internal Initiatives

SM

- **Data Segmentation for Privacy Initiative**
 - Demonstration Planned 1st Q 2013
- **eConsent Trial Project**
 - Launch in October 2012
- **Mobile Device Portfolio**
 - Mobile Device Provider Education
 - Mobile Device Research Project
- **Guide to Privacy and Security of Health Information**
- **Provider and Staff Security Video Games**

Data Segmentation for Privacy Initiative Overview



Data Segmentation for Privacy Initiative

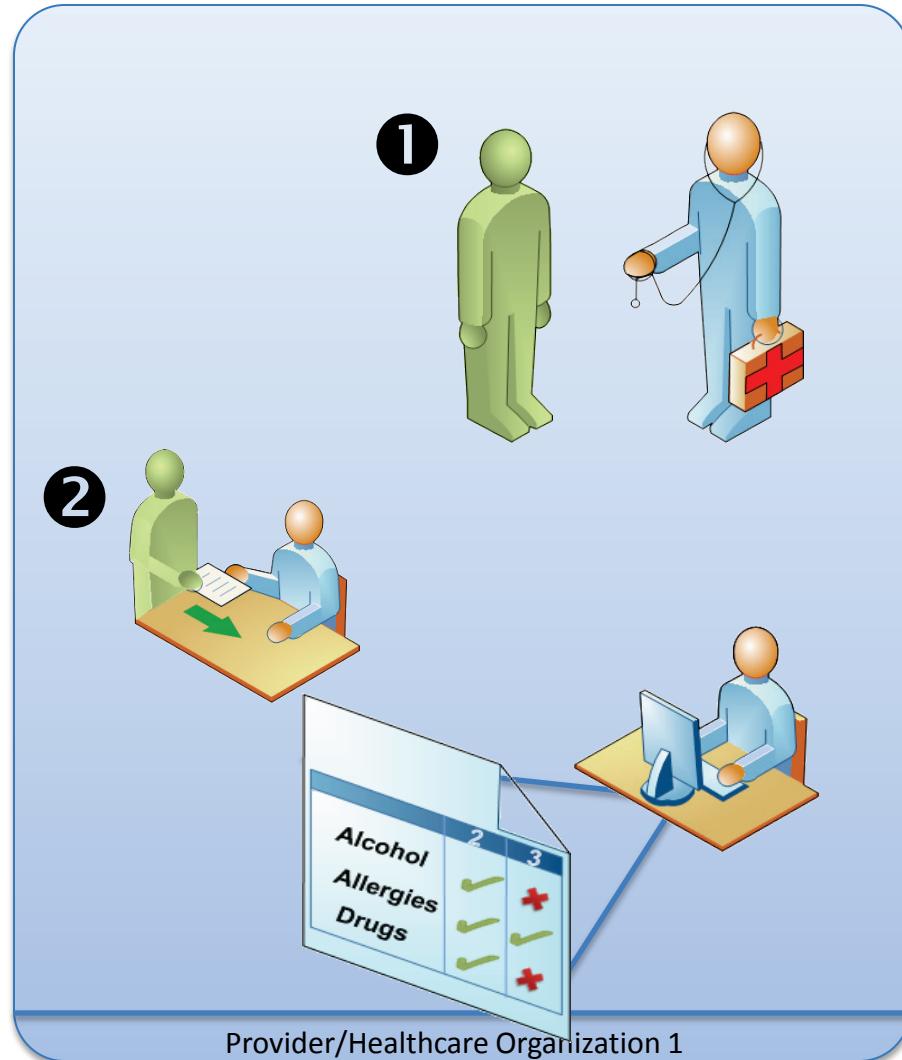
- Goal is to develop means to enable a patient to disclose some but not all of their health record

Project:

- Assessing and piloting metadata standards for sending some, but not all, of a medical record
- Marking information as not subject to re-disclosure without additional permission (in accordance with existing law)
- Partners: SAMHSA and Veterans Administration



User Story Example



- 1** The Patient receives care at their local hospital for a variety of conditions, including substance abuse as part of an Alcohol/Drug Abuse Treatment Program (ADATP).
- 2** Data requiring additional protection and consent directive are captured and recorded in the EHR system. The patient is advised that the protected information will not be shared without their consent.



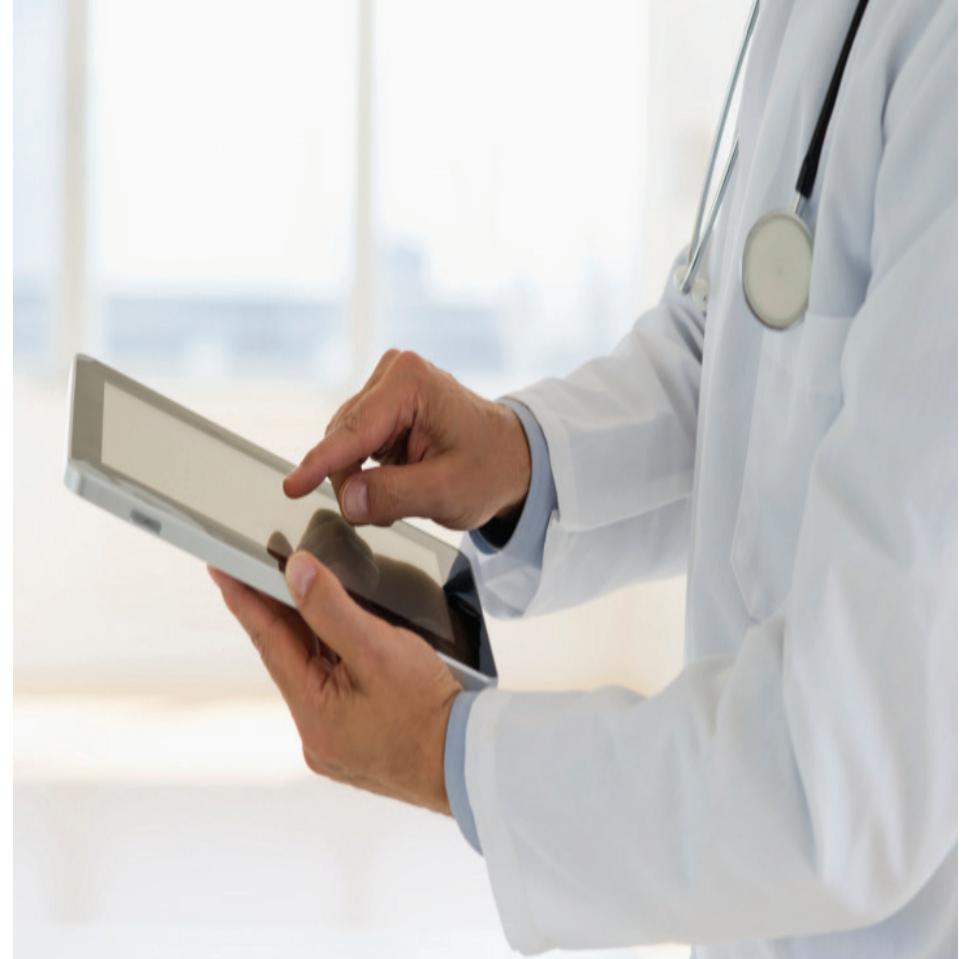
E-Consent Trial: Project Objectives

- **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 (Meaningful Choice)
 - Electronically obtain and record meaningful choice from individuals in a clinical setting.
- **Project Timeline: Pilot Launch October 2012**



Mobile Health

- 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 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
 - Timeline: November 2011 – October 2012

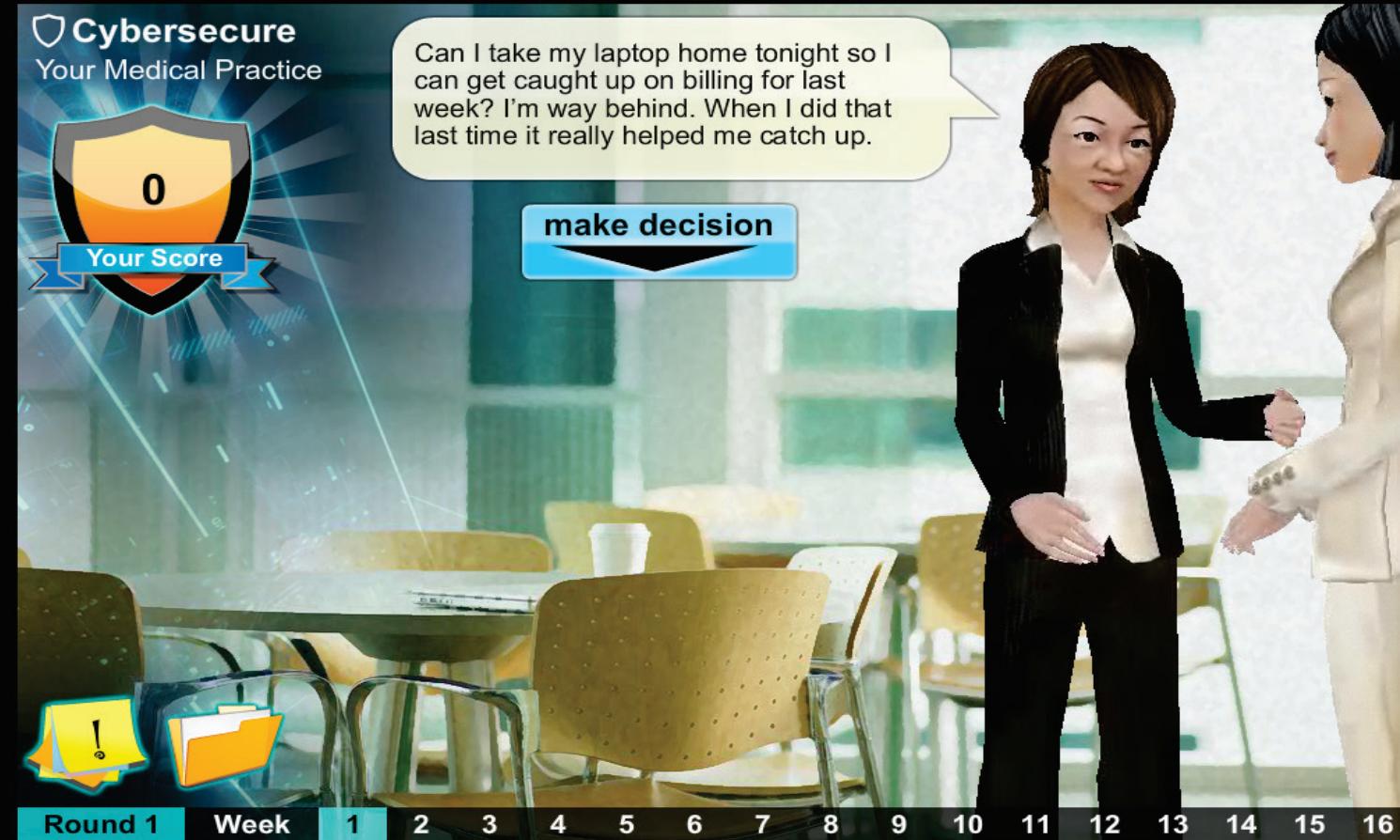
Helping Providers Integrate Privacy and Security into Their Culture



- 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
- Available at:
<http://www.healthit.gov/providers-professionals/ehr-privacy-security>

The cover of the booklet features a blue background with white diagonal stripes. At the top left is the logo for 'The Office of the National Coordinator for Health Information Technology'. At the top right is the logo for 'HEALTH & HUMAN SERVICES - U.S. DEPARTMENT OF'. The title 'Guide to Privacy and Security of Health Information' is centered in large, bold, blue capital letters. At the bottom left, it says 'Version 1.1 022312'. Below that, a small note reads: '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.' At the bottom right is the 'Putting the I in HealthIT' logo with the website 'www.HealthIT.gov'.

Training Materials: Security Video Game Released September 2012





We are all responsible for creating a culture
where *privacy and security are respected and
valued.*





QUESTIONS