Empowering Nurses & Building Trust Through Health IT

Helen Caton-Peters, MSN, RN
Health Information Privacy & Security Specialist
Office of the National Coordinator for Health Information Technology

#HealthIT4Nurses
Objectives

• Describe the roles of nursing, government, vendors, and patients in the development of a privacy and security culture that promotes trust

• Analyze recent HIPAA/HITECH and meaningful use privacy and security policy changes and their implications for practice

• Describe ways in which secure technology can address privacy and security challenges and contribute to empowerment of nurses and patients

• Discuss tools and strategies for sharing protected health information responsibly and securely
Privacy and Security: A Shared Responsibility

Health Care Providers
- Understand Rules
- Protect and Secure Information
- Educate Staff and Patients

Government
- Promotes Trust
- Develops Policies
- Fairly Enforces Rules

Patients
- Understand Rights
- Protect Personal Information
- Be Engaged

Technology Vendors
- Embrace Privacy by Design
- Provide Convenient Technology
- Implement Standards

#HealthIT4Nurses
Developing a Privacy & Security Culture

Challenges:

• Understanding new technology and privacy and security issues
• Reticence about asking questions or for assistance
• Difficulty in adopting new software and workflow in the fast-moving healthcare culture
• Adequacy of vendor training on privacy and security
What is Trust?

**Trust:** Firm belief in the reliability, truth, ability, or strength of someone or something.

– Oxford University Press
Americans’ Trust

More than 80% Americans rank nurses as having very high or high honesty and ethical standards.

<table>
<thead>
<tr>
<th>Professions</th>
<th>% saying “very high” or “high”</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nurses</td>
<td>82</td>
</tr>
<tr>
<td>Pharmacists</td>
<td>70</td>
</tr>
<tr>
<td>Grade school teachers</td>
<td>70</td>
</tr>
<tr>
<td>Medical doctors</td>
<td>69</td>
</tr>
</tbody>
</table>

– Gallup December 2013
Patient Trust

Ensuring privacy and security of health information including electronic health information is an important component of the clinician patient trust relationship.
Security incidents on the rise...

- Fourth Annual Benchmark Study on Patient Privacy & Data Security, Ponemon Institute, March 2014
84% of individuals either strongly agree or agree that health care providers have measures in place that provide reasonable protection for EHRs.
ONC Data Brief: Health care provider’s role in protecting EHRs

As confidence/trust about EHR protection falls, there is a corresponding increase/dramatic rise in the percentage of people withholding medical information.

![Bar Chart](chart.png)

- Strongly Agree: 4
- Agree: 7
- Disagree: 8
- Strongly Disagree: 33

#HealthIT4Nurses
HITECH Provisions

Expands individual rights and provides increased protection and control over PHI

- Restrictions on disclosures
- Information about services paid for out of pocket must be withheld from payers upon request
- TPO disclosures must be tracked and records maintained for three years
- CEs with EHRs must provide or transmit PHI in electronic format as directed by patient
- Sets limits for uses and disclosures for marketing and fundraising
- BA accountability
OCR HIPAA Audit Program

HITECH Act requires HHS to perform periodic audits to ensure CEs and BAs are complying with HIPAA Privacy & Security Rules.

OCR piloted a program to perform 115 audits of CEs to assess privacy and security compliance.

- Source: HHS Office of Civil Rights: June 2012
Meaningful Use

• Meaningful Use (MU): a set of measures which provides financial incentives when achieved by eligible providers and hospitals; EHR certification ensures the technology can support the requirements of MU

• Measures are designed to incentivize and reward providers and organizations for improved patient care through increased preventative care, care coordination, patient engagement and patient safety.

• CMS defines the EHR Incentive Programs; ONC defines the EHR Certification Criterion

• MU supports the HIPAA privacy and security rules, already a requirement for most providers
Objective: Protect electronic health information created or maintained by the certified EHR technology (CEHRT) through the implementation of appropriate technical capabilities.

Measure: Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the encryption/security of data stored in CEHRT in accordance with requirements under 45 CFR 164.312(a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the provider's risk management process for EPs.*

*42 CFR § 495.6(j)(16)(i)
Standards and Certification Criteria for EHRs

Privacy & Security Criteria

- Authentication, Access Control, and Authorization
- Auditable Events and Tamper Resistance
- Audit Reports
- Automatic log-off
- Emergency Access
- End-user Device Encryption
- Integrity
- Optional: Accounting of Disclosures
Current Issues in Nursing

Mobile Devices
Texting
Social Media
ONC Goal: Inspire Confidence and Trust

Promote the Secure Use of Health IT
- Information Assurance

Coordinate Development of Privacy and Security Policy
- Patient Direct Access to Lab Report (CLIA)
- Meaningful Use

Educate and Empower Patients and Providers
- Improved Access to Health Information
- View and Download Health Records
- Patient Education
- Enhanced Understanding of Patients

Provide Technical Assistance
- Interactive Security Training
- Data Segmentation for Privacy
- Notice of Privacy Practices
- eConsent Trial

#HealthIT4Nurses
Cybersecure: Contingency Planning

The latest training game focuses on disaster planning, data backup and recovery and other elements of contingency planning.

http://www.healthit.gov/providers-professionals/privacy-security-training-games
Coming Soon: Security Risk Assessment Tool

- Downloadable Risk Assessment Tool designed to guide providers through the Risk Assessment process.

- The tool includes resources to
  - understand the context of the question,
  - examples of potential impacts to PHI if requirements aren't met,
  - and includes actual safeguard language from the HIPAA Security Rule

Take the Steps to Protect and Secure Health Information when Using a Mobile Device

The resource center HealthIT.gov/mobiledevices was created to help providers and professionals:

Protect and Secure health information when using mobile devices

- In a public space
- On site
- At a remote location

Regardless of whether the mobile device is:

- Personally owned, bring your own device (BYOD)
- Provided by an organization
We’re All In This Together

Everyone has a role in protecting and securing health information
Comments or Questions?