Integrating Behavioral Health and HIV Into Electronic Health Records Communities of Practice

Monday, August 3, 2015
How to ask a question during the webinar

If you dialed in to this webinar on your phone please use the “raise your hand” button and we will open up your lines for you to ask your question to the group. (left)

If you are listening to this webinar from your computer speakers, please type your questions into the question box and we will address your questions. (right)

SESSION IS BEING RECORDED

Slides for today’s CoP are available on the CIHS website at:

Integrating Behavioral Health and HIV Into Electronic Health Records

Presented by: Adrian Bishop
Advocates for Human Potential

Agenda

- Introduction
- What is Cyber security and why is it important?
- Cyber security, HIPAA and personal health information
- Breaches
- Meaningful Use and HIPAA Security
- Data Sharing
- Resources and Links
Cyber security – why is healthcare vulnerable?

Exclusive: FBI warns healthcare sector vulnerable to cyber attacks (Reuters April 2014)

- Health data is far more valuable to hackers on the black market than credit card numbers because it tends to contain details that can be used to access bank accounts or obtain prescriptions for controlled substances.
- Demand for medical information, however, remains strong on criminal marketplaces, partly because it takes victims longer to realize the information has been stolen and report it, and because of the different ways the information can be used.
- Cyber criminals were getting paid $20 for health insurance credentials on some underground markets, compared with $1 to $2 for U.S. credit card numbers prior to the Target breach, according Cyber security firm Dell SecureWorks.
- Some criminals use medical records to impersonate patients with diseases so they can obtain prescriptions for controlled substances.

Reported Data Breaches in 2013 (By Industry / Entity)
How Does This Affect Us?

By the Numbers – Breaches of over 500 records (2014 Redspin, Inc.):

- 804 breaches of protected health information since 2009
- 29,276,385 patient health records affected by breach since 2009
- 7,095,145 patient health records breached in 2013
- 137.7% increase in the number of patient records breached in 2012-2013
- 85.4% percent of the total records breached in 2013 resulted from the 5 largest incidents
- 4,029,530 records breached in the single largest incident

How Does This Affect Us?

- 83.2% of 2013 of patient records breached in 2013 resulted from theft
- 22.1% of breach incidents in 2013 resulted from unauthorized access
- 35% of 2013 incidents were due to the loss or theft of an unencrypted laptop or other portable electronic device
- ~ 20% of PHI breaches have involved a business associate each year from 2009-2013
What is a Breach?

Compromises the security and privacy of the PHI” means that the breach poses a “significant risk of financial, reputational or other harm to the individual.”

What is Cyber Security?

Cyber security refers to preventative methods used to protect information from being stolen, compromised or attacked. It requires an understanding of potential information threats, such as viruses and other malicious code. Cyber security strategies include:

- identity management,
- risk management and
- incident management.
HIPAA, HITECH and Meaningful Use

Prior to HIPAA there were no universal standards for PHI.
• Compliance and Enforcement limited.

HITECH (part of the American Recovery and Reinvestment Act) broadened scope of HIPAA and increased enforcement.
• Breach notification and penalties.

CMS Meaningful Use incentive program mandated proof of compliance to HIPAA Security Rule.

ARRA – HITECH
2009

Meaningful Use
Guidelines for EHR
2010

Cyber security and HIPAA (Health Insurance Portability Accountability Act)

Focuses on the right of an individual to control the use of his or her personal information:
• Protected health information (PHI) should not be divulged or used by others against their wishes.
• Covers the confidentiality of PHI in all formats including electronic, paper and oral.
• Confidentiality is an assurance that the information will be safeguarded from unauthorized disclosure.

Focuses on administrative, technical and physical safeguards specifically as they relate to electronic PHI (ePHI).
• Protection of ePHI data from unauthorized access, whether external or internal, stored or in transit, is all part of the security rule.
• Covers
  • Computer Equipment
  • Any kind of removable/transportable digital memory media
  • All transmission media used to exchange information
What is Protected Health Information (PHI)?

This information is any individually identified health information including demographic information that relates to the individual's past, present, or future physical or mental health condition or any other identifying information that can be used to identify the individual:

- Names
- Address (including zip code)
- Dates (birth, admission, discharge, death)
- Telephone numbers
- Fax numbers
- E-mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/License numbers
- Vehicle identifiers and serial numbers (including license plate)
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) addresses
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code.

Need to Know

Minimum Necessary and Need to Know

The PHI you need to do your job is called "minimum necessary." It is information you "need to know" to do your job. Despite safeguards and controls to minimize access, we know that PHI surrounds us. If you come into contact with PHI and your job does not require it, you should not discuss or use this information.
Breaches

Definition of Breach

- A breach is an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information.

Reporting of Breaches

- **Individual.** Covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information within 60 days.

- **Notice to the Secretary.** In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of breaches of unsecured protected health information. Covered entities will notify the Secretary by visiting the HHS web site ([http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruc tion.html](http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruc tion.html))

- 500 or more records. Reported within 60 days. Less than 500 records may be reported at the end of the calendar year.

Breach Notification Penalties

<table>
<thead>
<tr>
<th>Violation Category</th>
<th>Each Violation</th>
<th>Violation Cap.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did not know</td>
<td>$100-$50,000</td>
<td>$1.5 million</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$1000-$50,000</td>
<td>$1.5 million</td>
</tr>
<tr>
<td>Willful neglect/corrected</td>
<td>$10,000-$50,000</td>
<td>$1.5 million</td>
</tr>
<tr>
<td>Willful neglect/uncorrected</td>
<td>$50,000</td>
<td>$1.5 million</td>
</tr>
</tbody>
</table>
HHS Wall of Shame

Location of Breached Information

- Laptop: 25%
- Desktop Computer: 20%
- Portable Electronic Device: 15%
- Paper: 10%
- Server: 5%
- Email: 5%
- Other/Unknown: 0%

HHS 2010 data
Data Breaches by Type

- Data stolen
- Data disclosed without authorization
- Data compromised by hackers
- Data lost
- Improper disposal of data
- Other

HHS 2011 data

Meaningful Use and HIPAA

Core Objective
- Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.
- 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.
# HIPAA

**Security Components** | **Examples** | **Examples of Security Measures**
--- | --- | ---
Physical Safeguards | • Your facility and other places where patient data is accessed  
• Computer equipment  
• Portable devices | • Building alarm systems  
• Locked offices  
• Screens shielded from secondary viewers
Administrative Safeguards | • Designated security officer  
• Workforce training and oversight  
• Controlling information access  
• Periodic security assessment | • Staff training  
• Monthly review of user activities  
• Policy enforcement
Technical Safeguards | • Controls on access to EHR  
• Use of audit logs to monitor users and other EHR activities  
• Measures that keep electronic patient data from improper changes  
• Secure, authorized electronic exchanges of patient information | • Secure passwords  
• Back-up data  
• Virus checks  
• Data encryption
Policies & Procedures | • Written policies and procedures to assure HIPAA security compliance  
• Documentation of security measures | • Written protocols on authorizing users  
• Record retention
Organizational Requirements | • Breach notification and associated policies  
• Business associate agreements | • Agreement review and updates

---

**Surviving a HIPAA Privacy/Security Audit**

The HHS Office of Civil Rights expects in 2015 to begin a random audit program to assess compliance with the HIPAA privacy, security and breach notification rules. At the HSGMA Conference, David Nattrass, a former senior advisor at OCR and now vice president of compliance services at security firm Cynegist, walked through what providers should expect for an audit.
HIPAA 2012 Audit Security Rule
Findings & Observations

Resources

HIPAA
- http://www.hhs.gov/ocr/privacy/

Wall of Shame (Breaches)
- https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Meaningful Use
- http://www.healthit.gov/policy-researchers-implementers/meaningful-use-regulations
3rd Session

Monday, August 31, 2015, 1:00 PM ET

Presenter Contact Information

• Adrian Bishop
  Advocates for Human Potential
  abishop@ahpnet.com

Additional Questions?
Contact Victor Ramirez
vramirez@mayatech.com
MAI-CoC CoP Listserv

- Subscribe: 
  http://nationalcouncilcommunities.org/read/all_forums/subscribe?name=integrating_ehrs_mai_coc

- Post to the list-serv: 
  Integrating_EHRs_MAI_CoC@nationalcouncilcommunities.org

For More Information & Resources

Visit www.integration.samhsa.gov or 
e-mail integration@thenationalcouncil.org
Thank you for joining us today.