You Keep Your Patients Safe. But Are They Secure?

Speaker(s):  Cynthia Krafft, PT, MS  
Walter Krafft, BS Electronic Engineering  
Sherry Teague, PTA, AT

Session Type:  Educational Sessions  
Session Level:  Multiple Level

This information is the property of the author(s) and should not be copied or otherwise used without the express written permission of the author(s).
You Keep Your Patients Safe, But Are They Secure?

Walter Krafft – ITIL Expert
Sherry Teague – MESS, ATC, PTA, HCS-D, HCS-O
Cindy Krafft – PT, MS, HCS-O

Session Learning Objectives

• Discuss the historical perspective of data privacy and security.
• Assess risk areas present during routine collection and use of patient information.
• Analyze real-life examples of risk specific to the delivery of home health services.
• Establish a plan for next steps to ensure data management is secure.

Disclosures

• Speakers do not have any relationships that could reasonably be viewed as creating a conflict of interest, or the appearance of a conflict of interest, that might bias the content of the presentation.
• No relevant financial relationships exists, but there is a personal relationship between two of the speakers ☺
Safety
• the condition of being protected from or unlikely to cause danger, risk, or injury.

Security
• the state of being free from danger or threat.

Setting Impact
What Data is out there?

What can they possibly know about me?

Breaches

• http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
What do those breaches cost?

- $217*
- $363*
- $28,070*
- $3,790,000*

*Ponemon Institute Research Report - 2015

How did the data breach?

- Malicious: 47%
- Human Error: 28%
- System Glitch: 25%

Who Cares?

- Internally – Employees, Leadership
- Externally – Consumers, Business Partners, Investors
Who's Problem is it?
Get Everyone Involved

- Privacy Professionals
- Security Professionals
- Company Executives
- Lawyers
- All Employees

How do I prevent a breach from occurring?

Privacy - Definition

“Privacy encompasses the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure and destruction of personal information.” The American Institute of Certified Public Accountants (AICPA)
Lifecycle of Data

Collection → Use → Retention → Disclosure → Destruction

Security

Intersection of Privacy and Security

Security – Control Types

- Preventative
- Detective
- Corrective
Security

• Access Controls
  – Authentication
    • Multi Factor
    • Biometric
  – Authorization
• Can be applied at many layers

Security

• Encryption
  – At rest
  – In Transit
  – Devices
  – Record Level
  – Field Level
  – File
  – Disk

Security

• Auditing and Monitoring
Security
Masking and Obfuscation

- Masking – Hiding portions of a field
- Obfuscation – Changing the contents but maintaining its utility

---

Security

- How much Security is too much?

---

Zero Trust Model

*Forrester Research*
Cloud Computing Implications and Considerations

- SLA’s – Service Level Agreements
- Physical Security
- Physical and Logical Sharing
- Access
- Encryption
- Internet of Things
- Location Based Services

Texting
E-mails

Could I be violating HIPAA?
- Sharing Logins
- Shoulder Surfing
- Talking too Loud
- Using the same password
- Family

Agency Case Study
Small to Medium Agency Dilemma
Case of “Many Hats”

- Very frequently small to medium agencies have few office personnel who wear many hats (for example: Director of Rehab is also acting HR and computer trainer)
- There is less office space—therefore less physical security
- All positions must be “revenue producing” therefore there could be assistance from several to do one job
- Passwords and access are spread across the office in order to increase efficiency

Physical Security

- Who gets past the front desk?
- Who “mans” the front desk?
- Is front area secured at all?
- Where is data stored? On site? Off Site?
- Are open office space computers secured?
- Are employees aware of EMR onlooker security?

HIPPA

- Do small and medium agencies name a HIPPA security officer?
- Do you inservice on HIPPA?
- What steps should you take if there is a breach?
- Example:
  Airborne charts
Employee Buy in

• Should involve EVERY employee
• Staff level committee and review
• Updating devices and new info education

Audit Toolkit

• Privacy Rule Assessment
• Security Rule Assessment
• Privacy Impact Assessment

Security Awareness Assessment

• Who’s around me?
• How am I connecting to the internet?
• Am I connecting via a secure connection? SSL HTTPS
• What happens when I click “send”?
• What happens to the information when it gets to the destination?
• Can the information be completely deleted?
Privacy Checklist

- Has your organization designated an Information Privacy and Security Officer?
- Have you developed a Notice of Information Practices to post in your office and distribute to each patient?
- Have you gathered, reviewed and compared your current forms, policies, and procedures to the HIPAA Privacy Regulations and State Privacy Regulations?
- Have you developed policies and procedures that meet the needs of your Human Resources Department with regard to Privacy requirements for the protection of health information of your staff?
- Have you developed processes for documenting, retaining, distributing and discarding Protected Health Information (PHI) as required by HIPAA?
- Have you developed processes for receiving, investigating and documenting individual complaints?
- Have you developed or revised current consent forms for patients in line with HIPAA regulations?
- Do you have all forms that must be read and signed by patients in languages appropriate to their culture?

Security Checklist

- Has your organization completed a Security Evaluation on the information systems used in conjunction with maintaining your current and future Protected Health Information?
- Does your organization have virus checking software, firewalls and operating systems that provide encryption and other security measures?
- Does your organization perform back-ups of your data daily?
- Does your organization have a Disaster Recovery and Contingency Plan to meet the HIPAA Security Standards?
- Has your organization developed security policies and procedures with regard to confidentiality statements, individually identifying information system users, passwords, automatic logoff, acceptable use, e-mail, internet usage, authentication of workstations, monitoring and documenting unauthorized access, audit trails of users, sanctions for misuse or disclosure and termination checklists?
- Has your organization provided for the overall physical security of your information systems, facility, staff, and medical records?
- Has your organization developed job descriptions for HIPAA required positions and all other positions in your organization?

Questions
Additional and Contact Info

- www.iapp.org
- www.ponemon.org
- www.forrester.com
- www.dwt.com/HIPAAtoolkit

Contact Information

- Walter Krafft:
  - wkraft@yahoo.com
- Sherry Teague:
  - teague@valuebeyondthevisit.com
- Cindy Krafft:
  - kraft@valuebeyondthevisit.com