Top10 Cyber Safety Rules

Rebecca Snell

DANKMEYER
PROSTHETICS & ORTHOTICS

Rule #1- Actual Rules

You know what they say, ignorance of the law is. no excuse.

- Health Insurance Portability and Accountability Act (HIPAA) 1996 & the Security Rule 2003
- Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009
- ABC Certification – Patient Records section
- https://www.healthit.gov/topic/privacy-security-and-hipaa

Rule #2 – Education!

Educating yourself and your staff is the #1 way to prevent cyber disasters.

Employee error is the leading cause of errors. And most errors are not malicious, but are unintentional.

EVERYONE IN THE COMPANY

OWNS THE SECURITY

OF THE COMPANY

Let’s review some vocabulary!

Required V. Addressable

Required means by law, we have to deal with it.

Addressable means that we can determine whether or not the standard is a "reasonable appropriate safeguard in the CE's environment." Factors include cost, size, technical infrastructure and resources.

At the very least, we must have done the analysis to determine if we are capable of doing something or not.

Compliance Officer

Also known as a Security Officer.

A large part of the HIPAA process is not just taking action, but documenting what you have done and what you will do.

THIS IS REQUIRED!!! You need one and everyone in the company needs to know who that is.

BUSINESS ASSOCIATES

As defined by HIPAA, a business associate is any organization or person working in association with or providing services to a covered entity who handles or discloses Personal Health Information (PHI), or Personal Health Records (PHR).

What about your EMR software vendor? Your suppliers? What level of security do they claim to have?

What is a breach?

- "An incident in which sensitive, protected or confidential data has been potentially viewed, stolen, or used by an individual unauthorized to do so. Data breaches may involve personal health information (PHI), personally identifiable information (PII), trade secrets or intellectual property." *WhatIs.com*
- "The intentional or unintentional release of secure information to an untrusted environment." *Wikipedia*
- For PHI - Any impermissible use or disclosure of PHI.

ran·som·ware
ˈransəmˌwer/
Noun

noun: **ransomware**; noun: **ransom-ware**

a type of malicious software designed to block access to a computer system until a sum of money is paid.

Disaster Recovery

Having a plan ready to ensure continuity of business operations in the event of a disaster.

That disaster could be physical – fire, flood, wind, etc.

That disaster could be a data breach.

FYI – REQUIRED

Rule #3 – Assess what you have to protect!

- REQUIRED
- What types of data are important, and why?
- Where is that data located?
- What types of losses present a significant risk to the company?

Don’t delay – time is $. Some solutions are obvious, easy and cost effective.

How much is it worth to you?

- PROTECTED HEALTH INFORMATION = ?? $$
- PAYROLL = ?? $$
- BANKING = ?? $$
- EMPLOYEE DATA = ?? $$
- LEGAL = ?? $$
- RESEARCH = ?? $$

Where is Your Data?

- Location:
  - Servers
  - Laptops
  - Accessible by personal devices
  - "The cloud" (Don't accept this as an answer: further define)
  - Hard copy data – paper files
  - Third parties (vendors; third party administrators)
- Type
  - At rest or in motion?
  - Encrypted or unencrypted?
  - Who owns it?
  - Format

Rule #4

How about
a
backup????

Could be the last resort.

Rule #5 – Physical Tools

Firewall

System patches/updates current

Anti-virus

Encryption

Secure email/text

Shredder

Alarm system

Firewall

- Software on your device limiting access to your hardware resources.
- A physical device that is a bulwark between you and your internet provider. Also controls access into and out of the network. Encryption available. Secured with password.

Anti-Virus and more….

Software on your device that looks for viral intrusions, malware, encrypts, password generator, checks websites for errors, …..

Rule #6 – HR Tools

- Employee Education
- Need to know
- Computer Policy and expectations
- A culture of awareness – social engineering

Employee: Phishing/Spearphishing

- Phishing: Impersonal “blast” email
- Spearphishing: Uses personal information about “sender” or recipient to encourage recipient to trust the email
  - Vacation plans
  - Recent promotions
  - Company events
  - Hobbies
- This information is all too easy to find: in f

Employee: Malicious and Negligent Conduct

- Departing employees
- Saving data on mobile storage devices
- Shadow IT (performance issues may encourage this behavior)
  - Saving Information Locally
  - Employee Cloud Storage
- Lost devices
- Weak passwords

Rule #7 – Passwords and ID

National Institute of Standards and Technology (NIST)

Have a password system.

Biometrics

2 Factor Verification (2FV): knowledge (something the user and only the user knows), possession (something the user and only the user has), and inherence (something the user and only the user is).

2 Step Verification (2SV): something the user knows and a repeat back

Passwords and ID – Why they fail

Annoying

Inconvenient

Too many of them

Change too often

Differing rules between logins

Rule #8 – Have a Breach Team and Plan

- NOT an IT problem
- Multidisciplinary planning team
  - Senior management/sponsor
  - IT
  - Legal
  - Human Resources
  - Risk Management
  - Business units
  - Public Relations

Breach Plan

- Plans executed on the fly usually don’t go well.
- Not all kinds of breaches require the same response.

Biggest Mistakes in Fire Control:

- Failure to plan
- IT takes control
- Lack of centralized control
- Self-investigation
- Delay

Key Steps

- Identify live vs. historical
- Isolate
  - Do not turn-off, power down, log in
- Gather and preserve other evidence (e.g. logs)
- Contact counsel
- Counsel hires external forensics
- Appoint a leader
- Gather a team

Incident Declaration

- Date
- Time
- Level
- Ongoing or contained
- Key contacts
- Detection method
- Systems affected
- Data affected
- Mode of attack
- Impacts
- Next steps

Rule #9 – Beware public WiFi

- Not secured.
- You don’t know who else is on, who set it up, and who might be monitoring data.
- Use a secure VPN to connect first.

Rule #10 –Be aware of social media!

- Be careful what you share.
- Monitor you/your kids' accounts.
- Remember Yahoo and Facebook disasters.

With thanks for breach material from:

Armstrong
Teasdale