Information Security in a HIPAA World

June 2018

navitend
GREENER GRASS THIS WAY

Introductions & Expectations

HIPAA Basics

Information Security Basics

HIPAA Gameplan

Q & A

Mission

(or Why this matters)

We have a **moral obligation** to those we serve – it is not only the law, but also out of respect for our patients and clients that we take this seriously.

Office of **Civil Rights** is responsible for enforcement.

Money Calibrates

Financial Costs

IT support & Data Forensics

Legal Fees

Cost to notify patients/clients

Credit Monitoring

Fines/Penalties/Settlements

Time Costs

Drama!

Communications internally and externally.

Unplanned work – never welcome.

Reputational Cost

Existing patients and clients may choose to depart.

New clients choose to go somewhere else.

Patient Info is a High-Value Target

Identity Theft

Fraudulent Tax Returns

Credit Scams

Insurance Fraud

Blackmail!

You can cancel a credit card, but you cannot cancel your medical information.

Vulnerabilities

Lost or stolen equipment which is not encrypted

Insider theft

Ransomware (now a reportable breach)

Publication/distribution

Poor legal guidance related to participating in medical research projects

Lack of Business Associate Agreements

Social media

You can cancel a credit card, but you cannot cancel your medical information.

Over 20 Years

1996 Portability of Health Insurance Information

2003 Privacy Rule

2006 Security Rule

2009 HITECH, Meaningful use accountability & Breach Reporting

2013 Latest (and final ?) rulings. Covered Entities == Business Associates

Like many pieces of legislation, the rules are written but the market changes.

We are all interpreting the rules and applying them to our present reality.

Privacy Rule

This protects the patient's right of who can access medical information.

Limited to medical advisement team.

Unless specifically granted, it does not extend to "research".

Exposure: Typically 1 at a time

Security Rule

Concerned with the Confidentiality, Integrity and Availability of electronic patient information.

Exposure: Thousands at a time

Reporting Rules

> 500 records

Patients, Government, Local Media (!) within 60 days

Smaller Breaches

Patients within 60 days

Government annually

Myth Busting

My organization is too small

My EHR vendor has this covered

My EHR (etc) is in “the cloud”

My Patient data is ONLY in my EHR

We purchased a HIPAA manual (still on bookshelf)

We are HIPAA certified

We have Cyber Security Insurance

Risk

CIA

Compliance

Basics of Information Security

AAA

Defense in Depth

Data Owner
Data Custodian

How ?

Controls

Administrative
Technical
Physical

Controls in Action

Project / Initiative / Risk	Administrative	Technical	Physical
Passwords	Establish requirements for complexity, expiration of passwords, maximum attempts to login.	Implement desired policy via domain level Group Policy	
Unattended computer security	Establish requirements for screen locking when machine is idle (Five Minutes).	Implement desired policy via domain level Group Policy	Mitigate risk of unauthorized access of computer terminals.
Terminal Server exposed to Internet	Establish policy of minimum requirements for accessing terminal server	Lock down firewall ports. Establish Virtual Private Network (VPN)	Must be on the campus or an authorized VPN user to access server.

Project / Initiative / Risk	Administrative	Technical	Physical
Printer Segregation	Establish role based security with appropriate groups and memberships. Identify which printers each group is permitted to use.	Implement desired policy via domain level Group Policy. A User's group membership dictates which printers are available.	Constrain printer utilization by location as well as group to minimize unauthorized printing / data loss.
Security Risk Assessment	Security Officer to oversee audit and follow through on recommendations based on the technical findings.		
Wi-Fi Networks	Establish usage policy.	Separate wireless networks to prohibit guests from accessing phone and corporate networks.	

Project / Initiative / Risk	Administrative	Technical	Physical
Email Server migration to improve security, reliability, availability, functionality and cost	Procure appropriate service from cloud vendor (Microsoft Office 365 and Google)	Migrate email from internal exchange server to Microsoft cloud solution.	Due to reduction in inbound internet traffic from relocated email server, this reduces localized power and internet outage concerns.
Email Retention Policy	Determine the retention requirements of email.	Enable “Litigation Hold” feature on Office 365 account.	
Email Encryption	Work with Security Officer to classify the email traffic which should be encrypted based on email content (keywords) and specific types of users.	Implement rules to implement encryption according to established policy.	

Project / Initiative / Risk	Administrative	Technical	Physical
HIPAA Business Associate Agreements (BAAs)	Establish Business Associate Agreements with appropriate vendors.		
Employee training	Require appropriate staff to take training.		
Backup Appliance	Classify data and define required backup sets. Identify required backup and disaster recovery solution to meet requirements.	Install, configure and deploy hardware and software to meet defined requirements. Monitor each business day and remedy issues asap.	Localized storage mitigates against local hardware issues. Remote file and virtualization capability mitigates against sustained internet and power outages.

Project / Initiative / Risk	Administrative	Technical	Physical
Privacy filters			Procure and install privacy screens on all relevant monitors.
Mobile Device Management	Establish a workable Bring Your Own Device (BYOD) policy as well as general mobile device usage policy.	Implement Mobile Device Management platform software.	
Mobile Device Encryption	Classify mobile devices to determine which devices store or access ePHI.	Encrypt appropriate mobile devices as a preventative measure against potential breach due to theft or accidental loss.	

Project / Initiative / Risk	Administrative	Technical	Physical
Perimeter security: Intrusion Prevention and Detection System (IPDS) Penetration Testing (pen test)	Annual Pen Test is recommended.	Select and implement IPDS	
Onboarding and Offboarding of employees as it relates to Information Security	Annual review of procedures both in their definition and a review of their execution.		
Proventiv Security Training	Proactive training to raise awareness, knowledge and skill in protecting organization information and patient information.	Training videos Periodic, targeted “phishing” emails to identify any individuals clicking on suspect email links.	

Project / Initiative / Risk	Administrative	Technical	Physical
Website	Content Management Sites (i.e. Wordpress) should not permit login without a digital certificate to encrypt traffic.	Install digital certification to enable TLS traffic.	
Unsupported Operating Systems (XP, Server 2003, etc)	Do not permit unsupported hardware and software to operate on the network without exceptional circumstances.	Keep systems patched.	Conduct a periodic inventory of all equipment and versions.

HIPAA Security Cheat Sheet

- Appoint a Compliance Officer
- Establish Business Associate Agreements
- Establish internal policies and procedures
  - Consistent and thorough training
  - Conduct Training *before* employees begin working
  - Documented sanction policy
- Conduct Annual Security Risk Assessment
  - Identify where PHI exists in your organization, including your “eco-system” of partners
- Risk Mitigation Plan
  - Take a low-drama approach to acting on the results of audit
  - Consult with Legal and Insurance teams to quantity and transfer risk, as appropriate
  - Establish a work plan
  - Work the plan
- Encrypt devices
  - Document this step and keep records current.
- Inventory all electronic assets
- Implement best practices around Authentication, Authorization, Auditing

Q & A

Now and/or Later

Frank Ableson, CISSP
CEO, navitend
fableson@navitend.com
www.navitend.com