PROTECTING THE CONSUMER'S FUTURE

NAHU

National Association of Health Underwriters

AMERICA'S BENEFITS SPECIALISTS

STEPS TO HIPAA COMPLIANCE: ELECTRONIC DEVICES OVERVIEW

About Your Presenter

David Smith
Vice President of Ebenconcepts , one of the Southeast's largest benefits consulting firms. He has nearly 20 years of experience in employee benefits with regulatory, business and industry perspectives. David has spoken extensively about wellness and its nuances and is always highly rated as a speaker before diverse audiences.

Who is Helping You With Security

Internal resource

- First step - complete Privacy and Security training

Outside vendor

- Look for an IT vendor, not a teenager or friend
- They must be HIPAA compliant
- Review their policies and procedures
- They must sign a subcontractor business associate agreement

The materials referenced here are subject to change, so frequent review of the source material is suggested.

What We Are Going to Cover

- Faxes
- Encrypting Email
- Data Encryption
- Password Protection
- Wi-Fi
- Website Security
- Backup
- Cloud Storage
- Firewalls
- Virus Protection
- Mobile Devices
- Remote Access
- Voice Mail
- Portable Storage Devices

Faxes

Faxes are not a secure way to transmit information

- Always use a cover sheet
- Secure fax machine
- Notify parties before sending faxes
- Send test fax before sending actual document
- If possible send information via more secure method
- Make sure fax machine isn’t saving any copies

If you use online fax program, a Business Associate Agreement is required

- Make sure they have a valid SSL license

Faxes with PHI sent to the wrong parties are considered a Breach and must be recorded and reported!

Email Encryption

- All PHI must be encrypted in transit, rest, and storage
- Review compliance plan
- 128-bit encryption or better
- Review for ease of use
- Business Associate Agreement is required with provider
- If you use a third party email provider, you must have a Subcontractor Business Associate Agreement

If an encrypted file is released, it is not a Breach

Hard Drive Encryption (Free)

For PC’s use BitLocker

- Windows 7 Enterprise and Ultimate
- Windows 8.1

For earlier PC Operating Systems

- DiskCryptor

Mac OS

- FileVault2

Password Protection

- First line of defense
- Make sure all devices have difficult passwords
  - 8+ characters with numbers, upper and lower case letters, and special symbols
- Require password changes frequently as described in your Policies and Procedures
- Make sure passwords are memorized or use password management software
- Password protect desktop, laptop, tablets and smart phones

Wi-Fi

- Encrypt network using WPA2 with Advanced Encryption Standard (AES)
- If you allow guests to access Wi-Fi use a guest portal
- Do not use factory supplied password for router
- Consider limiting router power so network doesn’t reach beyond your office

Website Security

- SSL/TLS License on site
- Force HTTPS on all pages to protect information
- Do not collect PHI through your website without proper protections
- Subcontractor BA Agreement with Web Host is required but not with transmission vendor (TWC, ATT, Verizon)

Backups

- Backups protect you from hard drive failures
- Backups need to be kept in a different secure location
  - Bank safety deposit box
  - Protect against theft, fire or flood
- Train multiple parties on how to perform a recovery of your computer systems
- Cloud – growing in popularity

Cloud Storage

- Review Cloud Storage Compliance Plan
- What level encryption do they use?
- Do they have access controls on data
- Audit trails?
- How do they get you back ups in the event of a failure?

Subcontractor Business Associate Agreement is Required

Virus Protection - Things to Look For

- Email Scanning
- Download Protection
- Spyware and Malware Scans
- Speed
- Compatibility
- Privacy Policy
- Real-Time Information
- Heuristic Analysis
- Automatic Updates

Mobile Devices

- Wireless calls are secure
- Critical that the devices are encrypted and password protected
- All SD cards need to be encrypted
- Update operating systems
- Install virus protection
- Text messaging is not secure unless you use a secure text messaging service (BAA Required)
- Enable tracking for all devices

If staff is supplying their own electronic devices implement a BYOD policy

Remote Access

Ability to access files and systems from outside the office

- Virtual Private Network

Cloud based solutions dominate

- HIPAA Compliant
  - ShareFile
  - Google Drive
  - Microsoft OneDrive
  - Box
- Not HIPAA Compliant
  - DropBox and iCloud

Voice Mail

- If voice mail is kept on computer as a part of your phone system you must physically secure the computer and encrypt the messages

- If a third party hosts your voice mail
  - Disable transcription service (Unless sent encrypted)
  - Disable emailing voice messages (Unless sent encrypted)

They must sign a Subcontractor Business Associate Agreement!

Portable Storage Devices

- Establish a policy on use of
  - USB Drives
  - Tablets
  - Portable drives

- Require that the data stored on these be password protected and encrypted

Staff Compliance is Key

- Employees compliance will determine the success of controlling the Protected Health Information your agency manages
- Employees should be trained to follow your compliance plan, and retrained annually

HIPAA Resources

www.TotalHIPAA.com/resources

- Email Encryption
- Cloud Storage
- Firewalls
- Secure Texting
- File Sharing
- Form Collection
- Consultants
- HIPAA Breach Insurance

TOTALHIPAA

COMPLIANCE

Affordable, Understandable, and Easy!

www.TotalHIPAA.com

800-344-6381

Use Coupon Code:
NAHU 10
Receive 10% Discount

QUESTIONS?