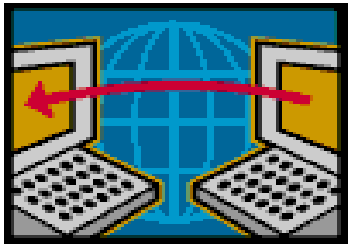
HIPAA SECURITY & SECURITY SAFEGUARDS

Presented by the Prospect Compliance and IT Departments

Overview

- HIPAA Security Rule
- Encryption v. Password Protection
- Recent Examples, Costs & Fines
- Your Role in HIPAA Security
- 10 Security Safeguards
- HIPAA & Social Media

HIPAA Security Rule



- Technical, physical and administrative safeguards to protect electronic protected health information ("ePHI")
- Confidentiality, integrity and availability of ePHI
  - Confidentiality: No disclosure of ePHI to unauthorized individuals or processes
  - Integrity: No unauthorized alteration or destruction of ePHI
  - Availability: ePHI accessible and usable on demand by authorized person

HIPAA Security Rule

- Two elements required for PHI:
  - Medical Information: Information related to a member’s past, present or future physical and/or mental health or condition, treatment or payment
  - Identifying Information: Includes at least one of 18 personal identifiers such as:
    - Account number
    - Name including initials
    - Dates of service
    - Full face photos
    - Other unique identifying characteristic

HIPAA Security

- Rule requires technical, physical and administrative safeguards to protect ePHI
- Technical safeguards:
  - Only authorized users access minimum necessary information to perform job
  - Ability to record and audit ePHI IT activity
  - Integrity & encryption of data in transmission

HIPAA Security

- Physical safeguards:
  - Limit access to places where ePHI stored
  - Safeguards for use and security of ePHI on desktops, laptops
  - Disposal and reuse of media with ePHI

HIPAA Security

- Administrative safeguards:
  - Risk analysis and risk management
  - Sanction policy
  - Information system audits
  - Security officer appointment
  - Ensure workforce access to ePHI appropriate
  - Security incident response team
  - Backups, disaster recovery and business continuity
  - Security & awareness training for workforce

HIPAA Security

- The administrative safeguard we’re focusing on this presentation:
  - Implement security & awareness training for workforce
    - Periodic security updates
    - Procedures for protecting against malicious software
    - Procedures for log-in monitoring
    - Procedures for creating, changing and protecting passwords

Encryption v. Password Protection

- If an encrypted device with ePHI is lost or stolen, it is usually not a reportable HIPAA breach
  - But if a password protected device with ePHI is lost or stolen it is usually a reportable HIPAA breach
  - This is so even if we remotely wipe the device
- Password protection is not encryption
- Encryption converts regular text into encoded text using an algorithm called an encryption key
  - Converting the encoded text back into regular text without the encryption key is very difficult
  - Keep the encryption key secure and separate; don’t keep it in writing near the device

Recent Examples

UCLA – May 2015 (but announced July 2015)

- Up to 4.5 million patients affected
- Names, addresses, dates of birth, SSNs, health information (all unencrypted)
- UCLA detected hacking activity since October 2014 but did not believe personal and medical information accessed
- Estimated total fines, credit protection, class action suits & IT fixes: $100 to $200 million

Recent Examples

Anthem – February 2015

- 80 million people across 14 states
- Names, birthdays, email addresses, SSNs (unencrypted), account numbers
- Hackers sent phishing emails with links to websites that looked like Anthem's (e.g., we11point.com) to get login information
- Estimated total fines, credit protection, class action suits & IT fixes: $1.5 billion to $3 billion

Recent Examples

Community Health Systems – August 2014

- 4.5 million people in 29 states
- Names, addresses, birth dates, telephone numbers and social security numbers
- User credentials obtained from device on network due to Heartbleed vulnerability; credentials used to obtain VPN access
- Estimated total fines, credit protection, class action suits & IT fixes: $75–$150 million

Recent Examples

- 1/3 Americans have been affected by health care security breaches
- Cyber criminals increasingly focused on health care information
  - Stolen debit and credit card information is perishable and has liability limits
  - Health care personal information can sell for 2 to 10 times the cost of retail information

HIPAA Fines and Penalties

Penalties can be imposed on entity or individual:

- HIPAA Criminal Penalties
  - Up to $250,000 fine and 10 years imprisonment
- HIPAA Civil Penalties
  - Up to $1,500,000 fine
- OCR Phase II Audits coming soon
  - OCR to select 350 providers to audit on privacy, security; failure may lead to corrective action plan
  - OIG has audited OCR and advocated enhanced enforcement
- Corrective and disciplinary actions for policy violations

Other HIPAA Security Breach Costs

- Other costs on top of fines/penalties:
  - Notices and credit monitoring
  - Media costs
  - Damage to reputation/lost business
  - Class action lawsuits
  - IT remediation
- Estimated costs of recent healthcare breaches
  - Average breach: $217 per member, $6.5 million overall

HIPAA Security – Your Role

- Security safeguards are only 10% technical
- 90% of security safeguards rely on user following good computing practices
- Review these security safeguards and understand them
- Ask questions if you don't understand security safeguards
- Report any suspected security incident

Ten Security Safeguards

- Unique User ID or Log-In
- Password Protection
- Workstation Security - Physical Security
- Security for Workstations, Portable Devices & Laptops with ePHI
- Data management, e.g., back-up, archive, restore, disposal

Ten Security Safeguards

- Secure Remote Access
- E-Mail Security
- Safe Internet Use
- Reporting Security Incidents/Breaches
- Your Duty to Follow Prospect HIPAA Security Policies & Procedures

#1 Unique User Log-In

- Each user gets a unique User ID to log-in
- Access to ePHI is appropriate and authorized
- Access is role-based
- Access is terminated for former employees
- Access is logged and audited

#2 Password Protection

- Use at least 8 characters and include at least 3 of the 4 following types of characters:
  - Uppercase & Lowercase letters (A-Z, a-z)
  - Numbers (0-9)
  - Special characters
  - Punctuation marks (!@#$%^&*())
- For brute force attack, hours to break 6 characters; weeks or years for 8 characters
- Try a “passphrase” to help you remember your password
  - Oscysbtdel76? (Oh say can you see by the dawn’s early light 76 ?)

#2 Password Protection

- Longer passwords are better
- Don’t use your user name as a password
- Don’t use “password,” “abcde,” proper names or dates
- Don’t share or reveal your password including to supervisors
- Don’t put a post-it stating “Password Reminder: XXX” near your desk or in your laptop bag
- Passwords must be changed when prompted every 90-180 days

#3 Workstation Security – Physical Security

- Workstation includes any electronic computing device that stores ePHI including laptops and desktops
- Physical security measures include:
  - Physical access controls
  - Device & media controls

#3 Workstations: Physical Access Controls

- Log off before leaving a workstation unattended
  - Unauthorized users won’t be able to access ePHI under your user ID
- Lock up: Offices, windows, workstations, sensitive papers, mobile devices
  - Lock your workstation
  - Lock up portable devices or take them with you
  - Don’t leave sensitive papers on printers/copiers

#3 Workstations: Device Controls

Unauthorized physical access to unattended device can result in modification of data, fraudulent email use, etc.

- Auto Log-Off: All devices must be configured to lock or auto log-off of applications and require a user to log on again if unattended for >5 minutes on average

#4 Security: Workstations & Portable Devices

Implement electronic security measures for workstations including:

- Up to date firewall and anti-virus software
- Install computer software updates
- Encrypt if possible
- Back up critical data and software programs
- Securely delete ePHI when no longer needed

#4 Security: Portable Devices & Media

- Portable devices and media include:
  - Smart phones
  - Memory sticks
  - External hard drives
- These devices pack big data in small packages
- They contain sensitive information which must be protected & pose a great risk for loss or theft

#4 Security: Portable Devices & Media

Safeguards for portable devices

- Don’t store ePHI on smart phones, memory sticks or external hard drives
- If you need to store ePHI on one of these devices, de-identify or encrypt
- Password protect portable devices
- Securely delete ePHI when no longer needed
- Back up original files
- Lock up these devices or keep them with you at all times

#4 Security: Portable Devices & Media

Safeguards for portable devices

- Don’t download information from your portable devices onto Prospect workstations or servers
  - Your information might have viruses or other malware
  - Ask IT before starting any such download
- Enable auto log off and screen lock
- Report to IT and Compliance immediately if any such device is lost or stolen

#4 Security: Portable Devices & Media

Recent Real Life Example

- Insurer Senior Health Partners contracted with Premier Home Health
- Premier nurse had encrypted laptop stolen from home with ePHI for 2,700 Senior members
- Laptop was encrypted but nurse wrote encryption key on laptop case
- Senior sent breach notifications to all 2,700 members; fines still pending

#4 Security: Portable Devices & Media

Real-Life Example

- Massachussetts dermatology practice staff had unencrypted thumb drive with 2,200 patients' ePHI stolen from car
- $150,000 HIPAA fine and corrective action plan

#5 Data Management & Security

- Data backup and storage
- Transferring and downloading data
- Data disposal

#5 Data Backup & Storage

- Store your sensitive information or ePHI on the shared drive
  - The shared drive (S or T drive) resides on the server, is secure and backed up
- Don’t store ePHI on your local drive on your workstation: not secure and not backed up
- Don’t store ePHI on portable devices like smart phones and memory sticks
- If you need to temporarily store ePHI on local drive, talk to IT regarding encryption

#5 Data Backup & Storage

Recent Real-Life Example

- Concentra had an unencrypted laptop with ePHI stolen from a physical therapy center
- Concentra had encrypted 400/600 laptops as of 2008 but then did nothing for 3 1/2 years
- $1.75 million fine and corrective action plan

#5 Transferring & Downloading Data

- Never transfer or download ePHI to your home computer or personal data storage (e.g., Dropbox, iCloud)
  - Your home computer isn’t encrypted
  - The storage vendors are not authorized to view Prospect’s ePHI

#5 Transferring & Downloading Data

- Health plans might request that you send files using FTP (file transfer protocol)
- But FTP is not encrypted and health plans will CAP us for transferring information using FTP
- Use FTPS or SFTP instead, both of which are encrypted
- Or encrypt the information before using FTP
- If you have questions, ask IT

#5 Clean Devices Before Recycling

Destroy ePHI when no longer needed

- Ask IT to “clean” hard drives, CDs, memory sticks before recycling or reusing

#5 Clean Devices Before Recycling

Recent Real-Life Example

- Health plan in New York returned copiers to leasing company without cleaning ePHI of 350,000 patients on copier hard drives
- CBS purchased one of the copiers and ran a story on it
- $1.2 million fine and corrective action plan

#6 Secure Remote Access

All remote access to ePHI must be encrypted

- Use your VPN or other secure connections
- Ask IT if this is unclear
- Ensure that others (e.g., business associates) also use secure connection for remote access

#7: Email Security

- When emails are in transit, they may pass through various systems or may never arrive at all
- Emails containing sensitive information or PHI need a higher level of security

#7: Email Security

- You don’t need to encrypt ePHI which is sent to other Prospect email addresses
- You do need to encrypt ePHI sent to any other address including our Hospital affiliates (e.g., Alta)
- Encrypt ePHI in transit by putting #secure# in title of email

#7: Email Security

- Never use your personal email to transfer or download ePHI
  - These transmissions are not secure or encrypted
  - The email vendors are not authorized to view Prospect’s ePHI either

#7: Email Security

Risk areas:

- Viruses. Malware that attaches itself to host file or program
  - User must execute the host file or program to activate the virus
  - Spread when user executes host file or program, e.g., opening an infected email attachment

#7: Email Security

Risk areas:

- Worms. Malware that is standalone
  - Not attached to a host program or file
  - Does not require user action to spread
  - Exploits vulnerability in targeted system or uses social engineering to trick user to execute

#7: Email Security

Risk areas:

- Trojan Horse. Hides itself in a harmless, helpful application but actually performs unintended or malicious function
  - Remains in a device and either damages it directly or permits someone at remote site to control it
  - Unlike viruses or worms does not infect other files on user’s system

#7: Email Security

- Viruses, worms, Trojan Horses can get on your device not just by email but also:
  - Websites like Google Hangouts and Linkedin
  - Unlicensed software
  - External devices like memory stick or portable hard drive

#7: Email Security

Risk areas:

- Phishing scams. Emails pretending to be from trusted organizations asking for password or other private information
  - Watch out for emails purporting to be from banks, government, news sources
- "Click this link" scams. Emails trying to trick you into clicking on a link that directs you to dangerous sites or compromises your computer
  - Check to see that the site is the real one, not the fake sites for Anthem and Premera

#7: Email Security

Risk areas:

- "Open or download this attachment" scams. Emails trying to trick you into opening or downloading a harmful attachment
- Spamming. Unsolicited bulk email including solicitations, advertisements, etc. May contain viruses, spyware, "scams" and slow down systems
  - Do not forward or reply to spam
  - Do not open spam
  - Prospect IT or management will never ask you for sensitive information like passwords via email or online

#7: Should I Open that Attachment?

- Don’t open a suspicious link such as:
  - Not work-related
  - Unknown link
  - Unexpected attachments
  - Attachments with a suspicious file extension (*.exe, *.vbs, *.bin, *.com, or *.pif)
  - Unusual subject lines: “Your car?”; “Oh!”; “Nice Pic!”; “Very Funny!”
- Notify IT right away

#7: Instant Messaging

Use caution with texts or Instant Messages ("IMs") to send sensitive information and ePHI

- Avoid sending ePHI or storing ePHI in texts
- Delete texts that are no longer needed
- Be aware that texts are subject to eavesdropping and snooping
- Texts on smart phones are especially dangerous if smart phone is lost or misplaced

#8: Internet Use

- Use responsible practices while online
- Don’t access sites from unknown links, or sites offering questionable content. This can lead to information theft, viruses or spam
- Don’t provide personal, sensitive or confidential information online
- Remember the Internet is not private and access to any Internet site can be traced to your name and location

#8: Internet Use

- Keep your browser updated
- Update your browsing applications, e.g., Adobe Flash, Acrobat
- Make sure web pages have https (not http) in the web address. The s stands for “secure” and tells you it’s encrypted.
- Don’t download questionable software or other media

#9: Security Incidents and ePHI

HIPAA defines “security incident” as

- “The attempted or successful improper instance of unauthorized access to, or use of information, or mis-use of information, disclosure, modification, or destruction of information, or interference with system operations in an information system.”

#9: Security Incidents and ePHI

- Report security incidents to IT which will share with Security Incident Response Team if necessary
- Report security breaches involving PHI to IT and Compliance
- Report any suspicious emails, unauthorized storage or transfer, possibly downloaded malware or sluggish workstation or other device
- React to IT notices re security incidents

#10: Duty to Comply with HIPAA Security Rule & Prospect Policies

You have a duty to:

- Review, understand and ask questions if you don’t understand anything this presentation, policies or IT notices
- Protect computer systems from unauthorized use or harm by using:
  - Common sense
  - Simple rules
  - Technology

Security Safeguards Summary

- Don’t share your user ID or password
- Select good passwords & keep them secure & safe
- Password protect your computer and portable devices
- Save your ePHI on the shared drive, not on your C:/ drive
- Securely delete ePHI when it is no longer needed

Security Safeguards Summary

- Logout and lock up or put things away before leaving an area unattended
- Use an encrypted laptop or memory stick if you must store ePHI on them
- Detect and report any suspected security incidents
- Practice good email and Internet usage and read and follow virus or other alerts from IT
- Ask questions to IT or Compliance

Sanctions for Security Violations

Workforce members who violate Prospect policies regarding IT security are subject to corrective and disciplinary action including:

- Termination of employment
- Civil lawsuit
- Criminal prosecution for HIPAA Violations

Quiz #1

HIPAA defines ePHI as:

1. Electronic personal health information
2. Electronic protected health information
3. Electronic protected hospital information
4. Electronic physical health information

Quiz #2

On which of these devices should you store ePHI on a long-term basis:

1. Home computer
2. Memory stick
3. Smart phone
4. Shared drive

Quiz #3

If you work with ePHI, which of the following safeguards are not required:

1. Store the least amount of ePHI as possible
2. Destroy ePHI when you are done using it
3. Do not use portable devices for long-term ePHI storage
4. Keep backup copies of ePHI in personal cloud storage, i.e., Dropbox

Quiz #4

Which of these are not among your duties related to IT security:

1. Understand and follow security rules
2. Report and respond to security incidents or breaches
3. Pick a password of sufficient complexity
4. Fix virus and malware problems on your own

HIPAA & Social Media

What is Social Media?

- Social Networks (Facebook)
- Blogs
- Chat rooms
- Third party rating sites (Yelp)
- Multimedia host sites (Youtube)
- Discussion Forums
- Collaborative Information/Publishing Systems (Wikipedia)

HIPAA & Social Media

Social Media Facts

- Posting PHI is almost always a HIPAA breach
  - The social media company, your friends, and your friends' friends have no right to view the PHI
- Even if the member is your social media friend or informally OK'd your post, that is not a formal HIPAA authorization
- Even if you didn't name the member, if you gave enough details so public could identify member, your post is PHI

HIPAA & Social Media

Social Media Do's

- Do use social media during your off-work time
- Do discuss the conditions of your employment
- Do exercise other rights protected by Section 7 of the National Labor Relations Act

HIPAA & Social Media

Social Media Don’ts

- Don’t use or disclose PHI or discuss members even in general terms on line
- Don’t post anything about work if you would be embarrassed if your supervisor found out

Questions?

- Call Hotline 1-877-814-9252

OR

- Call Compliance
  - Chief Compliance Officer, Hoyt Sze, 714-788-9711

OR

- Call IT help desk 562-293-3276`