HIPAA

Shweta A. Chawla
Founder & Investigator
SC Cyber Solutions

SC
Cyber Solutions

HIPAA

- Health Insurance Portability and Accountability Act (HIPAA)
- US federal legislation which addresses issues ranging from health insurance coverage to national standard identifiers for healthcare providers
- Deals with protecting the privacy and security of health data
  - Protected Health Information

shweta@sccybersolutions.com

SC
Cyber Solutions

What is Protected Health Information?

- Can be used to identify the patient
- Any information, transmitted or maintained in any medium, including demographic information
- Created/received by covered entity or business associate
- Relates to/describes past, present or future physical or mental health or condition; or past, present or future payment for provision of healthcare; and

shweta@sccybersolutions.com

SC
Cyber Solutions

Types of Data protected by HIPAA

- Written documentation and all paper records
- Spoken and verbal information including voice mail messages
- Electronic databases and any electronic information, including research information, containing PHI stored on a computer or other electronic device
- Photographic images
- Audio and Video recordings

shweta@sccybersolutions.com

SC
Cyber Solutions

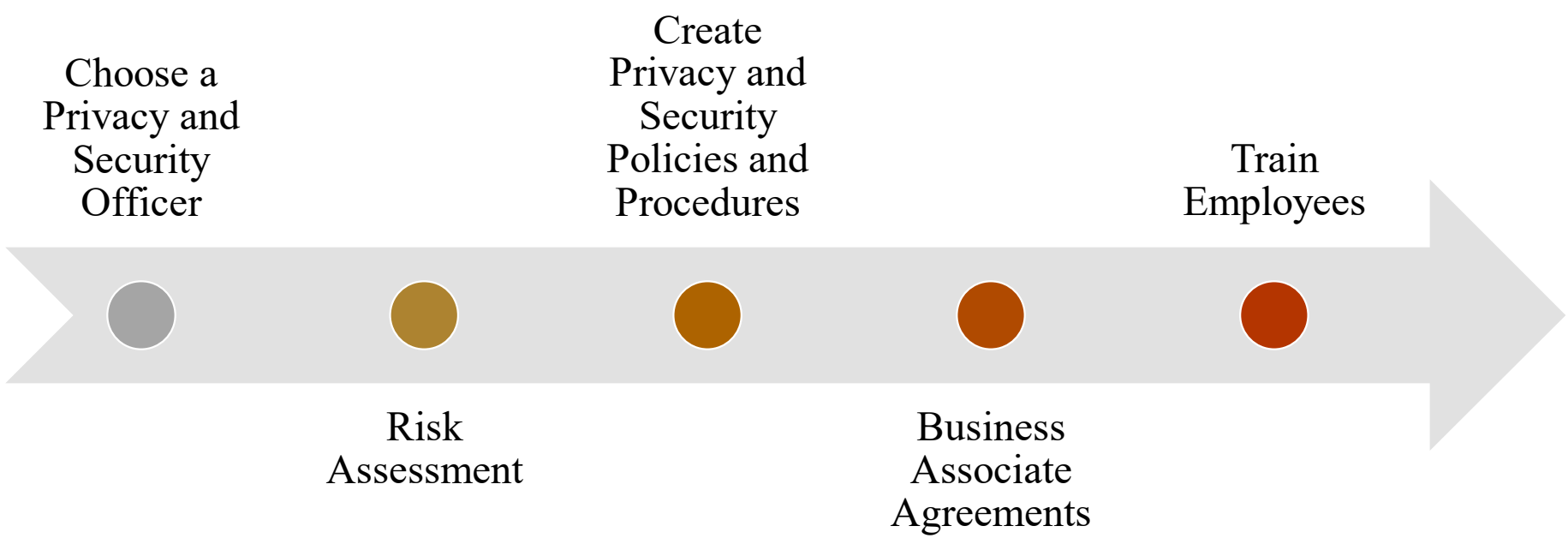
18 identifiers

- Names
- Geographic information smaller than state (address, city, county, zip)
- All elements of DATES (except year) including DOB, admission, discharge, death, ages over 89, dates indicative of age
- Telephone, fax, SSN, VIN, license plate
- Med record number, account number, health plan beneficiary number
- Certificate/license number
- Email address, IP address, URLs
- Biometric identifiers, including finger & voice prints
- Device identifiers and serial numbers
- Full face photographic and comparable images
- Any other unique identifying number, characteristic, or code

shweta@sccybersolutions.com

SC Cyber Solutions

Implementing HIPAA Compliance



shweta@sccybersolutions.com

SC
Cyber Solutions

Sanctions

- Disciplinary action against covered entities who fail to follow HIPAA rules
- Civil and/or criminal penalties including jail term

shweta@sccybersolutions.com

SC
Cyber Solutions

Covered under HIPAA

- Covered Entities
  - group health plans
  - physicians
  - hospitals
- Their Business Associates (their vendors)

- Employees of all the above

shweta@sccybersolutions.com

SC
Cyber Solutions

Disclosure of PHI

- To family / friends
  - Only PHI directly relevant to that person's involvement with the patient's healthcare or payment related to patient's healthcare
  - Only if the provider reasonably infers that the patient does not object.

shweta@sccybersolutions.com

SC
Cyber Solutions

Minimum Safeguard

- When HIPAA permits use or disclosure of PHI, a covered entity must use or disclose only the minimum necessary PHI required to accomplish the purpose of the use or disclosure.
- The only exceptions to the minimum necessary standard are those times when a covered entity is disclosing PHI for the following reasons:
  - Treatment
  - Purposes for which an authorization is signed
  - Disclosures required by law
  - Sharing information to the patient about himself/herself

shweta@sccybersolutions.com

SC
Cyber Solutions

Rules for Protecting Information

- Do not allow unauthorized persons into restricted areas where access to PHI could occur.
- Arrange computer screens so they are not visible to unauthorized persons and/or patients; use security screens in areas accessible to public.
- Log in with password, log off prior to leaving work area, and do not leave computer unattended.
- Close files not in use/turn over paperwork containing PHI.
- Do not duplicate, transmit, or store PHI without appropriate authorization.
- Storage of PHI on unencrypted removable devices (Disk/CD/DVD/Thumb Drives) is prohibited without prior authorization. Consider using UA Box.

SC
Cyber Solutions

Encryption of PHI

- Electronic protected health information must be encrypted when stored in any location outside the EHR including desktops, laptops, and other mobile devices (thumb drives, CDs, DVDs, smart phones, email, cloud storage devices (e.g. UA Box), etc.).
  - Use of other mobile media for accessing and transporting PHI such as smart phones, iPads, Netbooks, thumb drives, CDs, DVDs, etc., presents a very high risk of exposure
- Use of personal computers or other personal electronic equipment (non-UA owned equipment) is not allowed to store protected health information.

SC
Cyber Solutions

- Any exceptions must be approved by senior leadership or in compliance with your entity's portable device guidelines.
- Due to a lack of infrastructure and control of delivery, the use of unencrypted text messaging of any protected health information is strongly discouraged. Text messaging of medical orders is prohibited

shweta@sccybersolutions.com

SC
Cyber Solutions

Password Management

- Do not allow coworkers to use your computer without first logging off your user account.
- Do not share passwords or reuse expired passwords.
- Do not use passwords that can be easily guessed (dictionary words, pets name, birthday, etc.).
- Should not be written down, but if writing down the password is required, must be stored in a secured location.
- Should be changed if you suspect someone else knows it.

SC
Cyber Solutions

- Disable passwords or delete accounts when employees leave.
- Passwords:
  - Should be minimum 8 characters long
  - Include 3 of 4 data types (upper/lower case, numeric, special characters)
  - Should be changed periodically
  - Good password scheme is critical for complex passwords –

shweta@sccybersolutions.com

SC
Cyber Solutions

Protection from Malicious Software

- Malicious software can be thought of as any virus, worm, malware, adware, etc.
- As a result of an unauthorized infiltration, PHI and other data can be damaged or destroyed.
- Notify your supervisor, system support representative, and/or security officer **immediately** if you believe your computer has been compromised or infected with a virus—do not continue using computer until resolved.

SC
Cyber Solutions

- Managed anti virus and other security software is installed on all University computers and should not be disabled.
- Any personal devices used for access to PHI must have appropriate anti virus software .
- Do not open e-mail or attachments from an unknown, suspicious, or untrustworthy source or if the subject line is questionable or unexpected—DELETE THEM IMMEDIATELY.

shweta@sccybersolutions.com

SC
Cyber Solutions

Ransomware

- Ransomware is malicious software that denies access to data, usually by encrypting the data with a private encryption key that is only provided once the ransom is paid.
- Presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident.
  - Whether it results in an impermissible disclosure of PHI and/or a breach depends on the facts and circumstances of the attack.
  - When ePHI is encrypted due to a ransomware attack, a breach has occurred because the ePHI was acquired.

SC
Cyber Solutions

- Once the ransomware is detected, we must initiate our security incident response and reporting procedures.
  - If computer with encrypted data is powered on and the operating system loaded, the data is decrypted and breach notification may need to occur.
  - Notification of a breach of unencrypted or decrypted data must occur unless there is a "low probability the PHI has been compromised"
    - Maintaining frequent backups and ensuring ability to recover data from backups may show low probability (if no exfiltration of PHI).

shweta@sccybersolutions.com

SC
Cyber Solutions

Beware of Suspicious Emails

- Be very cautious of suspicious emails that request information such as email ID and password, or other personal information claiming that you need to verify an account, or you are out of disk space, or some other issue with your account.

SC
Cyber Solutions

Use of Technology

- Use of other mobile media for accessing and transporting PHI such as smart phones, iPads, Netbooks, thumb drives, CDs, DVDs, etc., presents a very high risk of exposure and requires appropriate authorization.
- Email, internet use, fax and telephones are to be used for UA business purposes (see UA policies).
- Fax of PHI should only be done when the recipient can be reliably identified; Verify fax number and recipient before transmitting.
- No PHI is permitted to leave facility in any format without prior approval.

SC
Cyber Solutions

- Where technically feasible, email should be avoided when communicating unencrypted sensitive PHI - follow your organization's email policy for PHI.
- No PHI is permitted on any social networking sites (Twitter, Facebook, etc.) without appropriate authorization.
- No PHI is permitted on any texting or chat platforms.
- If a situation requires use of email or text, appropriate encryption techniques must be used.

shweta@sccybersolutions.com

SC
Cyber Solutions

Rules for Disposal of Computer Equipment

- Only authorized employees should dispose of PHI in accordance with retention policies.
- Documents containing PHI or other sensitive information must be shredded when no longer needed. Shred immediately or place in securely locked boxes or rooms to await shredding.
- All questions concerning media reallocation and disposal should be directed to your HIPAA Security Officer; OIT systems representatives or your departmental IT support teams are responsible for sanitization and destruction methods.
- Media, such as CDs, disks, or thumb drives, containing PHI/sensitive information must be cleaned or sanitized before reallocating or destroying.

- "Sanitize" means to eliminate confidential or sensitive information from computer/electronic media by either overwriting the data or magnetically erasing data from the media.
- If media are to be destroyed, then once they are sanitized, place them in specially marked secure containers for destruction.
- NOTES: Deleting a file does not actually remove the data from the media. Formatting does not constitute sanitizing the media.

shweta@sccybersolutions.com

SC
Cyber Solutions

Reporting Security Incidents

- Notify your Security Officer of any unusual or suspicious incident.
- Security incidents include the following:
  - Theft of or damage to equipment
  - Unauthorized use of a password
  - Unauthorized use of a system
  - Violations of standards or policy
  - Computer hacking attempts
  - Malicious software
  - Security Weaknesses
  - Breaches to patient, employee, or student privacy

Contact details:
Mob: +91 98230 80864
shweta@sccybersolutions.com
www.sccybersolutions.com
@sccs1300