

Protecting Electronic Health Information

HIPAA Security Rule
Awareness and Training

Protected Health Information (PHI)

PHI includes any of these and more –

Name

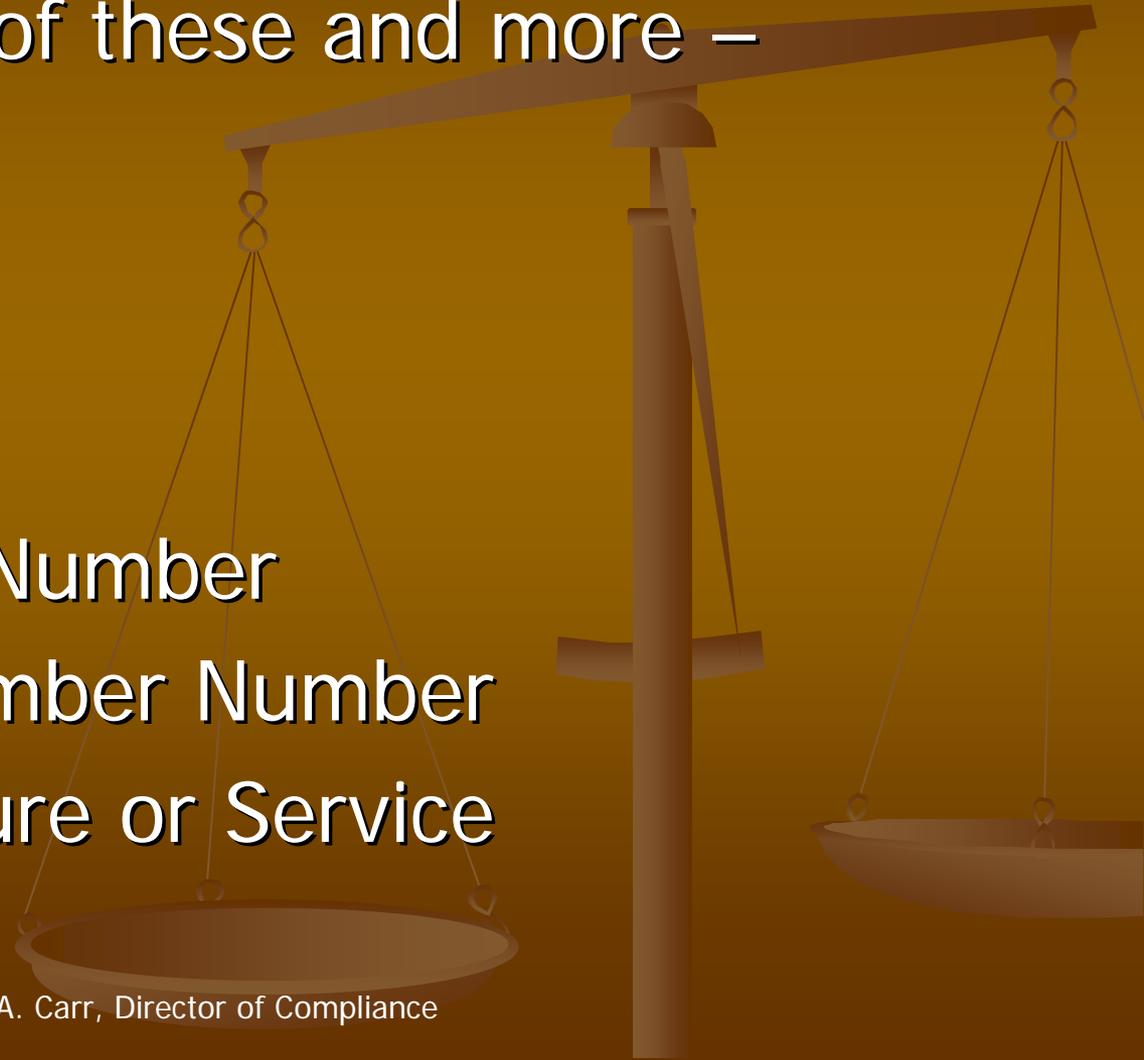
Address

Date of Birth

Social Security Number

Health Plan Member Number

Medical Procedure or Service



Privacy Rule

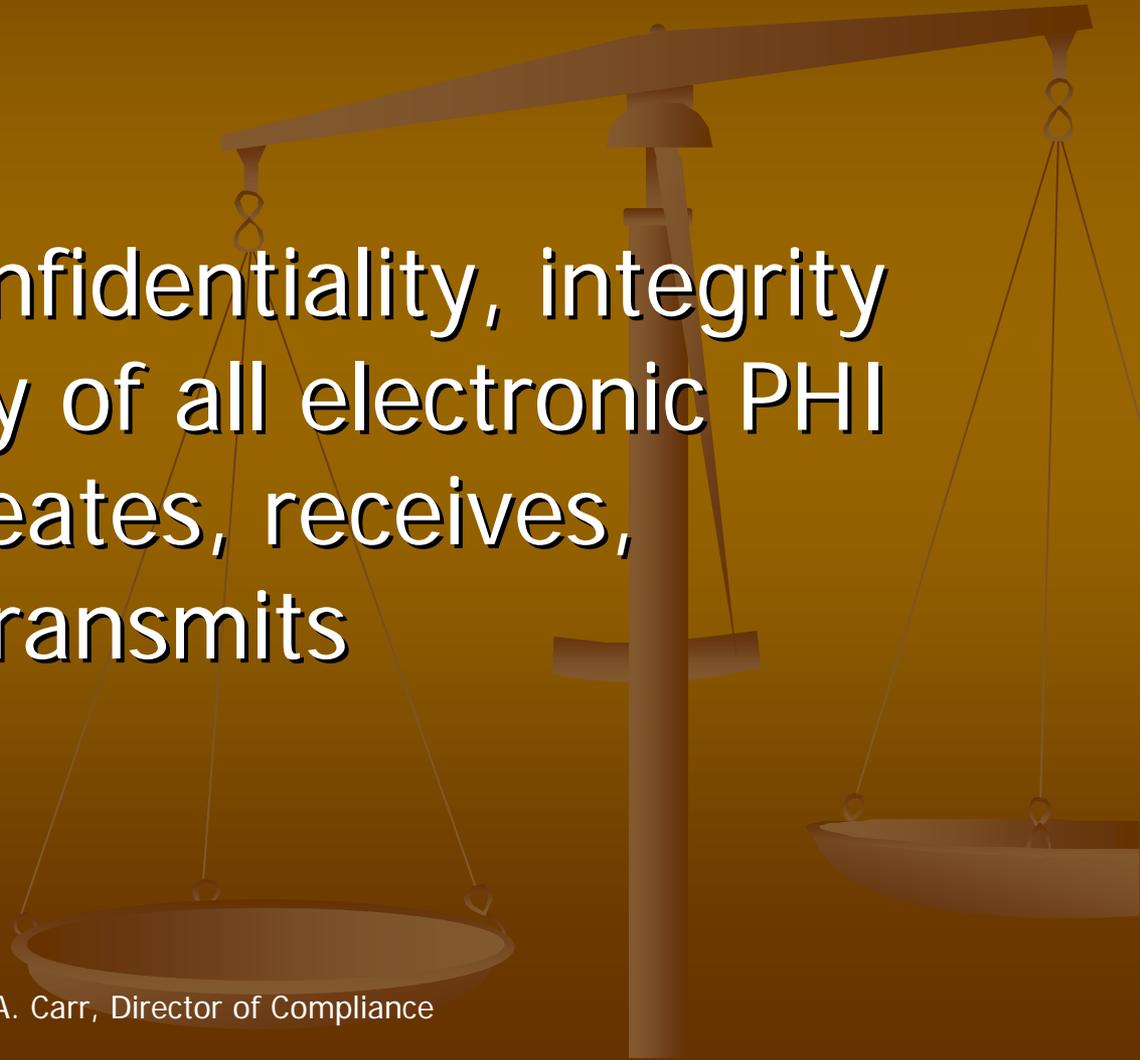
- The HIPAA Privacy Rule applies to protected health information in any format...
 - Written or Printed
 - Oral
 - Electronic

Privacy and Security Rules

- The Privacy Rule AND the Security Rule require administrative, physical and technical safeguards
- Privacy covers PHI in any format
- Security covers PHI only in electronic format

HIPAA Security Rule requires

- Ensure the confidentiality, integrity and availability of all electronic PHI the agency creates, receives, maintains or transmits



HIPAA Security Rule requires

- Protect against all reasonably anticipated threats or hazards to the security or integrity of such information



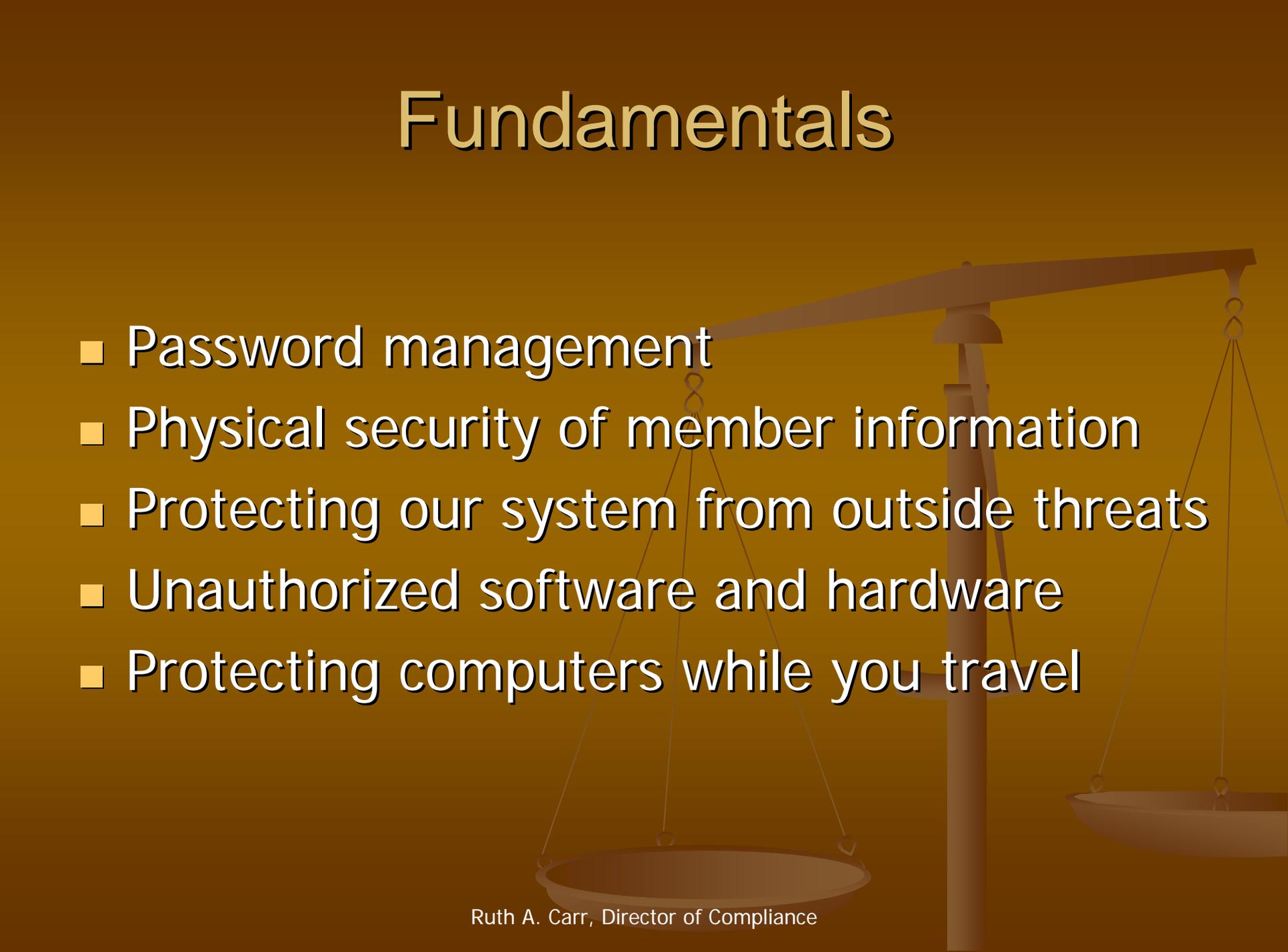
HIPAA Security Rule requires

- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted by HIPAA or required by law

HIPAA Security Rule requires

- Ensure that everyone complies

Fundamentals



- Password management
- Physical security of member information
- Protecting our system from outside threats
- Unauthorized software and hardware
- Protecting computers while you travel

Password Management

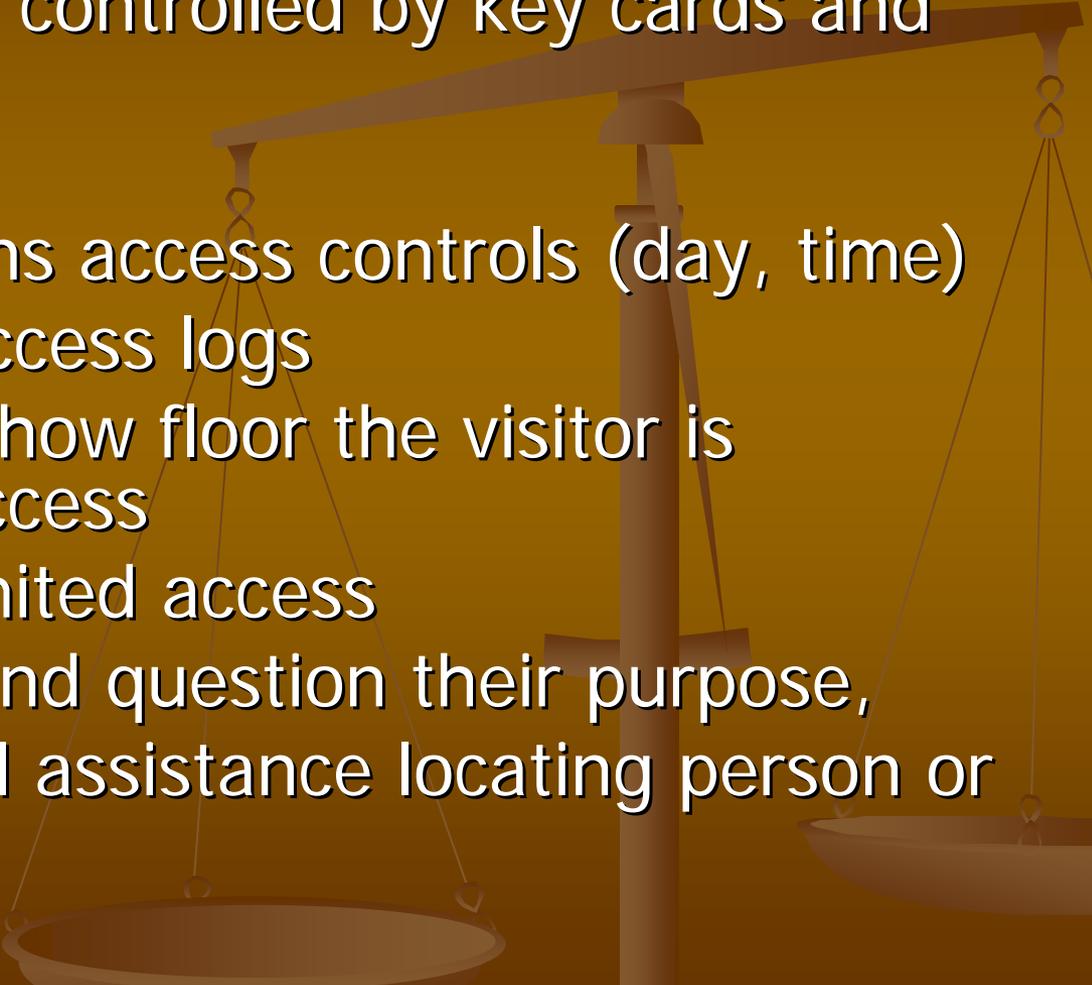
- HIPAA Security requires agency to have procedures for managing passwords
 - Details are set by agency, not by law
 - DCH requires strong passwords:
 - Include both upper and lower case letters
 - Include digits and special characters, as well as letters(0-9 and !@#\$%^&*{+?)
 - At least eight characters long
 - Expire every thirty days

Physical Security



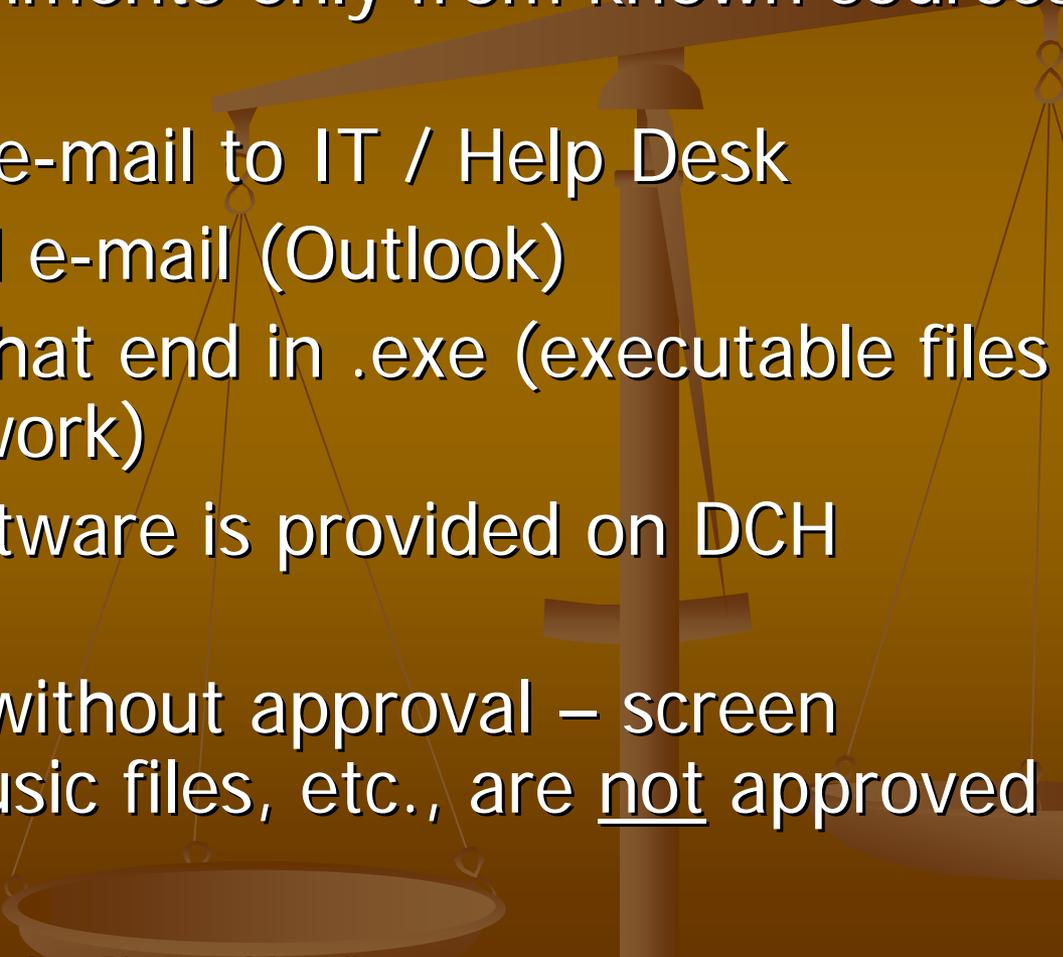
- Most common threat to security is people
- Wear identification badge
- Be sure doors close, not propped open
- Log-off when going away from computer
- Store records with PHI in closed area
- Shred or other destroy of records with PHI
 - Do not throw PHI in trash

Physical Security



- Premises access is controlled by key cards and alert staff
 - Agency maintains access controls (day, time)
 - Can generate access logs
 - Visitor badges show floor the visitor is authorized to access
 - Visitors have limited access
 - Notice visitors and question their purpose, ask if they need assistance locating person or room

Outside Threats



- Open e-mail attachments only from known sources / senders
- Report suspicious e-mail to IT / Help Desk
- Use only approved e-mail (Outlook)
- Be aware of files that end in .exe (executable files can harm the network)
- Virus scanning software is provided on DCH computers
- Do not download without approval – screen savers, games, music files, etc., are not approved

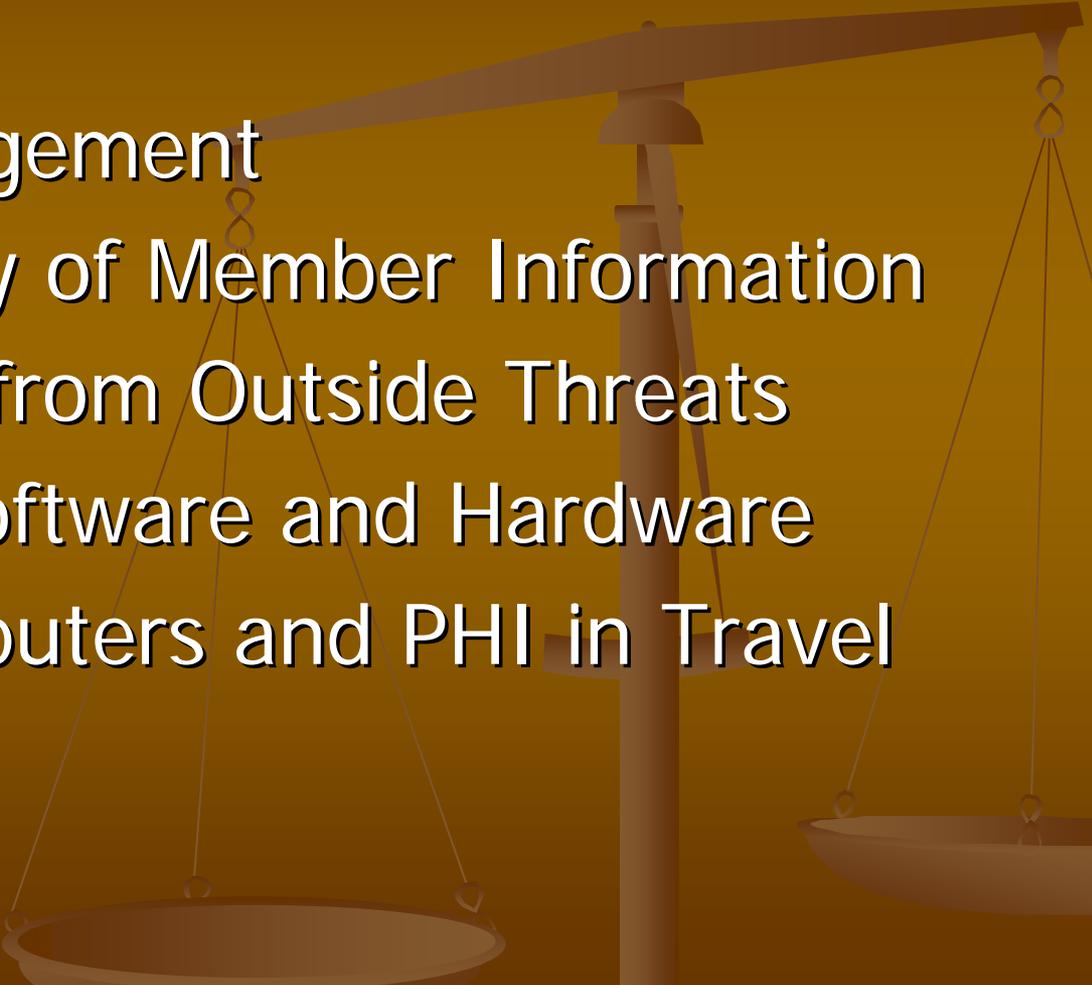
E-mail

- E-mail in a state agency is public record
 - Keep it short and smart
 - Limit copies to those who need to know
- No PHI is disclosed in public records
- Always "Send Secure" outside of DCH
- Limit copies and forwards to "need to know" basis
- Delete e-mail containing PHI as soon as it is no longer needed

Protecting PHI Out of the Office

- When you travel or work away, use added precautions with your laptop and PDA (BlackBerry, I-Phone, smart phones, etc.)
 - Lock PDA in drawer, briefcase
 - Notice your surroundings, visibility of screen
 - Password protect your BlackBerry
 - Do not keep passwords on PDA
 - Make sure your PDA's virus protection is in place and up to date

Summary



- Password Management
- Physical Security of Member Information
- Protect System from Outside Threats
- Unauthorized Software and Hardware
- Protecting Computers and PHI in Travel

Training



- Security Rule requires security awareness for entire workforce
- Privacy Rule and Security Rule require training in privacy and security policy and procedures for staff who work with PHI
- DCH HIPAA training will be available online
 - Staff can access training on their schedules
 - Resource materials available on Web

Security Awareness Test

Answer True or False:

- The Security Rule applies only to PHI in electronic form (e-PHI) sent in DCH e-mail. _____
- The Rule does not require availability of e-PHI. _____
- The greatest threat to security is people. _____
- The Rule requires protection against any possible threats to security of information. _____
- The Rule requires strong passwords, encryption of e-mail and photo identification cards for staff. _____
- Training in privacy and security are optional. _____

Security Awareness Test

Answer True or False

- The Privacy Rule applies to electronic PHI. _____
- The Security Rule applies to printed PHI. _____
- Disclosure to any DCH staff member of a member's e-PHI is authorized. _____
- DCH staff may not use any e-PHI without the member's written authorization. _____
- DCH must do whatever is necessary to guarantee confidentiality of e-PHI. _____
- E-mail is secure if a disclaimer or confidentiality notice appears at the end. _____

HIPAA Security Awareness

- Questions?

