
HIPAA Information Security Training

1. Health Insurance Portability and Accountability Act (HIPAA)

- *Administrative Simplification*
 - o Transaction code standards (November 2003)
 - o Privacy (April 2003)
 - o **Information Security (April 2005)**

2. What needs to be protected?

- **Protected Health Information (PHI)**
Health or medical information linked to a specific individual:
 - o Identity – **demographic and financial data**, and
 - o Medical condition and treatment – **clinical data**
- **Electronic Protected Health Information (EPHI)**
PHI stored on or transmitted via our computers and networks, including CDs, PDAs, tapes, and clinical equipment

3. What is Information Security?

- **Confidentiality**
Prevent unauthorized access or release of EPHI
Prevent abuse of access (identity theft, gossip)
- **Integrity**
Prevent unauthorized changes to EPHI
- **Availability**
Prevent service disruption due to malicious or accidental actions, or natural disasters.

4. How is protection done?

- **Policies and procedures** (10 policies + Sanctions policy)
- **Infrastructure security**
 - Computer network and systems security
 - Physical security
 - Workforce security
 - Backup and Disaster recovery
 - Authentication and Termination
 - Authorization and Audit logs
- **Responsibilities**
 - User responsibility
 - Manager responsibility
 - Asset owner responsibility

5. USER Responsibility: *What are the consequences of security failure?*

- Disruption of patient care
- Increased cost to the organization
- Legal liability and lawsuits
- Negative publicity
- Identity theft (monetary loss)
- Disciplinary action

6. USER Responsibility: *What are the types of security failures?*

- **Intentional Attack**
 - o Malicious software (Bots, Spyware)
 - o Stolen Passwords (Keyloggers)
 - o Impostors calling or e-mailing to steal information (Phishing)
 - o Theft (Laptop, PDA)
 - o Abuse of privilege (Employee/VIP clinical data)
- **Employee Carelessness**
 - o Sharing passwords
 - o Not signing off the systems
 - o Downloading and executing software
 - o Sending EPHI outside the institution without encryption
 - o Not protecting PDA and Laptop with password and encryption
 - o Pursuing risky behavior – Improper web surfing, and instant messaging
 - o Not questioning or reporting suspicious or improper behavior

7. USER Responsibility: *How do we protect against such failures?*

- Install anti-virus, anti-spyware solutions, **install security patches, update daily.** **Use caution** when viewing web pages, e-mail attachments, and using games and programs.
- **Chose strong passwords** with non-dictionary words, 7 characters and longer, mix alpha-numeric letters, **refuse to share it**, change if you suspect a breach.
- Protect your laptop or PDA **with a password**, and **turn on encryption** on sensitive folders, including copies in CD, USB storage devices, etc.
- **Do not abuse clinical access privilege**, report if you observe an abuse (if necessary, anonymously).
- Do not be responsible for another person's abuse by neglecting to sign off, this negligence may easily lead to **your suspension and termination.**
- **Do not copy**, duplicate, or move EPHI without a proper authorization.
- Do not email EPHI without encryption to addresses outside the institution.
- Strictly follow principles of '**Minimum necessary**' and '**Need-to-know**' – the 3 fundamental missions of the institution are **Care, Research and Education.**

- **Challenge improper behavior**, question suspicious behavior, report violations and security problems to proper authorities – email to hipaa@columbia.edu or security@cumc.columbia.edu or call CUMC IT Helpdesk (305-HELP).
- Communicate with colleagues and staff about secure and ethical behavior.

8. MANAGER Responsibility: *What security measures are expected within a group?*

- Be aware of EPHI access patterns and methods by the managed workforce based on their job function’s “need-to-know.” **Understand and discuss the authorization definitions** that are used to provide access in necessary EPHI applications. **Demand to know and follow the documented steps** to provide necessary access when a workforce member joins the institution.
- **Communicate and reinforce USER Responsibility** towards Privacy and Security of EPHI with the managed workforce in group meetings.
- **Follow workforce clearance procedures** for temporary and private workforce members, and **promptly request termination of (or change in) all accounts** of a departing workforce member (or a member whose job responsibilities are changing) by **making it a clear and definite step** within the termination (or separation) process.
- In cooperation with the owners of the EPHI systems, **conduct access audits** on EPHI access and updates for the workforce to determine compliance.
- Analyze the physical layout of the managed environment to **implement optimal workstation placement** for managed workforce members for privacy and security.
- **Document change in operational processes** within the managed environment **addressing both short-term and long-term unavailability** of EPHI that is required operationally. Train the workforce on the changes.
- **Be vigilant**, challenge improper behavior compromising privacy and security, and report violations and security problems to proper authorities – email to hipaa@columbia.edu or security@cumc.columbia.org or call CUMC IT Helpdesk (305-HELP).

9. ASSET OWNER Responsibility: *How should security controls be implemented?*

- **Understand Information Security Policies and Procedures** thoroughly.
- Conduct Risk Analysis by **filling out Questionnaires** and by **documenting processes and procedures**.
- **Register the asset. Follow the documented processes. Conduct security audits. Reduce and manage risks by implementing security controls.**
- **Employ competent custodians** and administrators who are trained in management and security of the asset.
- **Do not be an asset owner if you are unable to measure risks and allocate resources to secure the asset.** Security risk analysis **should be done prior to acquiring an asset** for a full understanding of costs.