



University of Connecticut Health Center

FORM D
University of Connecticut Health Center
HIPAA SECURITY
QUICK REFERENCE GUIDE
2009 - 2010

What is HIPAA?

The Health Insurance Portability and Accountability Act is a federal law. HIPAA provides for:

- Enhanced privacy to protect individually identifiable health information (protected health information or PHI) in any form (oral, paper, electronic) and enhanced patients rights with respect to their PHI (effective April 14, 2003);
- Standard security measures to ensure confidentiality, integrity, and availability of data (effective April 20, 2005).

What is considered Protected Health Information (PHI) and Electronic Protected Health Information (ePHI)?

PHI Information is believed to identify an individual if it includes either the individual's name or any other information that could enable someone to determine the individual's identity. Protected Health

Information may include:

- Name and address
- Geographic identifiers such as address and zip code
- Telephone or fax numbers
- Health care specifics
- Social Security or medical records numbers

Examples of **ePHI** include any medium used to store, transmit, or receive PHI electronically, such as the following:

- Personal Computers with their internal hard drives used at work, home, or traveling
- External portable hard drives, including iPods
- Magnetic tape or disks
- Removable storage devices such as USB memory sticks/ keys, CDs, DVDs, and floppy diskettes
- PDA's, smart phones
- Electronic transmission includes data exchanges via wireless, Ethernet, modem, DSL or cable network connections.

Who does HIPAA Security apply to?

HIPAA Security standards apply to covered entities, such as the Health Center. A covered entity is a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA. HIPAA Security standards apply to all individuals who have equipment connected to the UCHC network. In addition, it applies to all individuals at UCHC, because as a member of the UCONN Health Center community you may come in contact with patient information.

What are HIPAA Security Standards?

HIPAA Security Standards are Federal rules that:

- Define administrative, physical, and technical safeguards to protect electronic protected health information.
- Require implementation and documentation of basic safeguards.
- Protect PHI currently or previously in electronic form.

How do I comply with the Security Standards? As a member of this community you must do the following:

- Always wear your Health Center Identification provided to you from the Department of Public Safety.
- Adhere to UCHC guidelines for creating appropriate passwords- see Policy Number 2005-05; if there are questions, see your systems administrator
- Memorize your passwords and log off your computer by using password-protected screen savers when you are not at your work station
- Do not use e-mail to send or transmit ePHI to internal or external recipients.
- If you receive an e-mail attachment from someone you don't know, don't open the attachment. And don't forward it to anyone. Instead, delete it and report it to your supervisor and the Help Desk.
- Unless authorized, never install any software on your computer.
- If you suspect that your computer may be infected with a virus, immediately report it to your supervisor and the Help Desk.
- Never load data files from outside CDs and diskettes without first scanning them for viruses.
- Back-up all data files containing ePHI and other sensitive information and encrypt and/or password-protect
- If using a mobile device, protect against unauthorized access by utilizing passwords and encryption
- Keep all file cabinets and rooms that contain PHI locked.

How do I comply with the Security Standards? As a member of this community you must do the following:

- Always wear your Health Center Identification provided to you from the Department of Public Safety.
- Adhere to UCHC guidelines for creating appropriate passwords- see Policy Number 2005-05; if there are questions, see your systems administrator
- Memorize your passwords and log off your computer by using password-protected screen savers when you are not at your work station
- Do not use e-mail to send or transmit ePHI to internal or external recipients.
- If you receive an e-mail attachment from someone you don't know, don't open the attachment. And don't forward it to anyone. Instead, delete it and report it to your supervisor and the Help Desk.
- Unless authorized, never install any software on your computer.
- If you suspect that your computer may be infected with a virus, immediately report it to your supervisor and the Help Desk.
- Never load data files from outside CDs and diskettes without first scanning them for viruses.
- Back-up all data files containing ePHI and other sensitive information and encrypt and/or password-protect
- If using a mobile device, protect against unauthorized access by utilizing passwords and encryption
- Keep all file cabinets and rooms that contain PHI locked.

HIPAA Security Standards:

HIPAA Security Standard	*See Our Policy and Procedure
<p>Administrative Safeguards:</p> <ul style="list-style-type: none"> • Assign security responsibility within the organization. • Develop policies and procedures to address security violations. This includes completing a risk analysis, implementing security measures to reduce risks and vulnerabilities, developing a sanction policy, and implementing procedures to review records of system activity on a regular basis. • Attend to workforce security including: workforce clearance procedures, termination procedures and authorization, and/or supervision of workforce and management. • Establish policies and procedures for granting access to ePHI. • Provide security awareness training to the workforce and management. • Identify and respond to security incidents. • Implementing policies and procedures for responding to an emergency: including plans to back up data, recover after a disaster, and operate during a disaster or emergency. • Periodically evaluate the organization's compliance with the Security standards. 	<p>Policy Number 2005-02: UCHC HIPAA Security Acceptable Use</p> <p>Policy Number 2005-03: UCHC HIPAA Security Administration</p> <p>Policy Number 2005-05: UCHC HIPAA Security Information Systems Access Control</p> <p>Policy Number 2003-09: Breaches of Privacy & Security of Protected Health Information (PHI): Reporting Requirements, Sanctions, and Mitigation</p> <p>Policy Number 2005-06: UCHC HIPAA Security Information Systems and Business Continuity and Disaster Recovery</p> <p>Policy Number 2003-07: UCHC Training of Workforce: HIPAA Privacy & Security</p>
<p>Physical Safeguards:</p> <ul style="list-style-type: none"> • Limited physical access to electronic information systems and the facilities in which they are housed. • Proper authorization for access. • Standards that ensure proper workstation use and physical security of workstations that access ePHI. • Standards for device and media controls. 	<p>Policy Number 2005-01: UCHC HIPAA IT Security: Data Authentication, Physical Safeguards</p> <p>Policy Number 2005-04: UCHC HIPAA Security Facility Access Control</p> <p>Policy Number 2005-10: UCHC HIPAA Security Virus Protection Policy</p> <p>Policy Number 2005-09: UCHC HIPAA Security Tracking and Disposal of Equipment and Electronic Media Containing ePHI</p>
<p>Technical Safeguards:</p> <ul style="list-style-type: none"> • Technical policies and procedures for access control on systems that maintain ePHI. These systems must allow for unique user identification and include an emergency access procedure for obtaining necessary ePHI during an emergency. Addressable specifications include automatic logoff and encryption and decryption. • Hardware, software, and/or procedural methods for providing audit controls. • Mechanisms to validate the ePHI has not been altered or destroyed in an unauthorized manner. 	<p>Policy Number 2005-01: UCHC HIPAA IT Security: Data Authentication, Physical Safeguards</p> <p>Policy Number 2005-07: UCHC HIPAA Security Information System Activity Review</p> <p>Policy Number 2005-08: UCHC HIPAA Security Risk Management, Evaluation and Audit</p>

POLICY NUMBER 2008-03

May 27, 2008

POLICY: MOBILE COMPUTING DEVICE (MCD) SECURITY

PURPOSE:

The University of Connecticut Health Center (UCHC) has established this policy for the secure implementation and deployment of mobile computing and storage devices within UCHC to support both privacy and security of sensitive information and compliance with applicable agency and regulatory requirements (e.g. HIPAA, NIH, HHS.)

SCOPE:

This policy applies to:

- Employees (including faculty and staff)
- Volunteers
- Residents
- Temporary staff
- Agency and contracted staff
- Credentialed staff
- Members of the Board of Directors

This policy covers portable or mobile computing and telecommunications devices (referred to as MCD's) that can execute programs or store data. Because all MCD equipment used at the Health Center is institutional property, regardless of funding source, this definition includes all UCHC laptop computers, PDAs, BlackBerry® devices, and USB storage devices.

DEFINITIONS:

Confidential or restricted data

Includes, but is not limited to, personally-identifiable information that is not in the public domain and if improperly disclosed could be used to steal an individual's identity, violate the individual's right to privacy or otherwise harm the individual. Organizational information that is not in the public domain and if improperly disclosed might: cause a significant or severe degradation in mission capability; result in significant or major damage to organizational assets; result in significant or major financial loss; or result in significant, severe or catastrophic harm to individuals. This data may include, but is not limited to: Mobile Computing Device Policy # 2008-03 (5/27/08)

- Student information
- Medical/Dental/Behavioral Health-related patient information (ePHI)
- Other sensitive Health Center information not in the public domain
- Financial information about the Health Center (budgets, strategic revenue plans, accounts receivable/payable details)
- Employee HR and financial information
- Any information about employees, students, patients, Board Members, etc. which includes Social Security numbers

- IDs and/or Passwords for access to Health Center computing resources
- Research data requiring protections (clinical trials, patient survey responses, etc.) as required by the NIH

POLICY STATEMENTS:

Permissible Use

UCHC confidential or restricted data is not authorized to be stored on a UCHC or non-UCHC MCD unless the criteria below are met:

1. The device stores only the minimum data necessary to perform the function necessitating storage on the device
2. Information is stored only for the time needed to perform the function
3. The device is encrypted using methods authorized by the UCHC IT Department
4. Data is protected from any and all forms of unauthorized access and disclosure

IT Responsibilities

1. The UCHC IT Department will provide Mobile Computing Device users with approved and properly updated software-based security mechanisms which may include anti-virus, anti-spyware, device locating, encryption, firewalls, and intrusion detection.
2. The UCHC IT Department will work with the Security Breach Team to establish, document, and maintain reporting, mitigation and remediation procedures for lost or stolen mobile devices containing UCHC data and for UCHC data that is compromised through accidental or non-authorized access or disclosure.

Mobile Computer Device User Responsibilities

1. Users may not bypass or disable security mechanisms under any circumstances.
2. Users in the possession of UCHC-owned mobile devices during transport or use in public places, meeting rooms and other unprotected areas must not leave these devices unattended at any time, and must take all reasonable and appropriate precautions to protect and control these devices from unauthorized physical access, tampering, loss or theft.
3. Unauthorized physical access, tampering, loss or theft of the device must immediately be reported to the UCHC IT Help Desk in order to initiate effective and timely response and remediation.
4. Basic Science users who do not store confidential or restricted data may optionally use the device encryption software provided and supported by the UCHC IT Department.

Governance

1. Failure to adhere to this security policy and associated procedures may result in sanctions as per applicable UCHC policy.

Sandra Armstrong (signed) June 16, 2008

Chief Information Officer Date

Peter Deckers, M.D. (signed) June 18, 2008

Executive Vice President for Health Affairs Date

Replaces Policy #2003-32 Originally issued 4/14/03

Updated: May 27, 2007

*The complete UCHC HIPAA Privacy Policies are available online at: http://www.policies.uchc.edu/area/HIPAA_Privacy.html.

*The complete UCHC HIPAA Security Policies are available online at: http://www.policies.uchc.edu/area/HIPAA_Security.html.

Who enforces the Security standards?

The center for Medicare and Medicaid Services within the U.S. Department of Health and Human Services will enforce the security standards.

Civil and Criminal Penalties

Congress provided civil and criminal penalties for covered entities that misuse personal health information. For civil violations of standards, Office for Civil Rights may impose monetary penalties up to \$100 per violation, up to \$25,000 per year, for each requirement or prohibition violated. Criminal penalties apply for certain offenses; up to \$100,000 and up to five years in prison if the offenses are committed under "false pretenses"; and up to \$250,000 and up to 10 years in prison if the offenses are committed with the intent to sell, transfer or use protected health information for commercial advantage, personal gain or malicious harm.

Who to Contact

If you believe privacy rights have been violated or that security breaches have occurred, these must be reported. UCHC Policy Number 2003-09 gives some examples of breaches of confidentiality and security (also known as **security incidents**). Other occurrences that may constitute a security incident are:

- a stranger using your computer
- odd behavior or degraded performance from your computer
- seeing information on your computer that you do not regularly have privilege to see
- data that suddenly changes for unknown reason
- missing files or unusual files appearing on your drive (server or hard drive)
- changes in access privileges
- suspected password compromise (activity showing up under your user id that you know you did not do)
- last network logon from your computer was not your user id

- For suspected PRIVACY rights violations, you must contact:

Iris Mauriello, RN, Corporate Compliance Integrity and Privacy Officer, at 860-679-3501 or mauriello@nso1.uchc.edu.

- For suspected SECURITY breaches you must contact:

The IT Help Desk at x.4400 or Jonathan Carroll, UCHC Information Security Officer, at 860-679-3528 or jcarroll@uchc.edu.

FORM D

*University of Connecticut Health Center
HIPAA SECURITY
QUICK REFERENCE GUIDE*

**Certificate of HIPAA Security Awareness
Training Completion**

I have read and understand the University of Connecticut Health Center's HIPAA Security Quick Reference Guide. Further, I understand that the full HIPAA Security Policies can be obtained from my department manager or found online at:

http://www.policies.uhc.edu/area/HIPAA_Security.html.

Your signature indicates that you have received, read, understood, and will abide by all the above information concerning HIPAA Security Standards.

Please return this form to either:

- your preceptor (if you are a student) for placement in your student file.
- HR (MC 1051) if you are an employee

Signature

Date Signed

Print Name

Department

Supervisor Signature

Date Signed

Print Name

Department

Reviewed 6/07, 4/08, 4/09