

## **MEMORANDUM**

TO: SIU School of Medicine Faculty, Staff, & Students

FROM: Sandra A. Walters, CIO, SIU P&S

RE: Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule

---

***“Confidentiality is everyone’s job, not everyone’s business.”***

This memorandum is designed to educate and/or remind all SIU faculty and staff concerning the Security Rule (*Federal Register: February 20, 2003 (Volume 68, Number 34), FR Doc 03-3877, 45 CFR Parts 160, 162, and 164, Pages 8334-8381*) portion of the HIPAA regulations administered by the Department of Health and Human Services, the proper safeguards for securing confidential electronic protected health information (ePHI), and highlights from SIU HIPAA Security Policies and Procedures. SIU is a covered entity under the HIPAA regulations since we handle ePHI.

The HIPAA Privacy Rule covers Protected Health Information (PHI) in all formats – verbal, written, *and* electronic. The effective date for the Privacy Rule was April 14, 2003. The HIPAA Security Rule requires additional protection and safeguards for electronic PHI (ePHI). The effective date for the Security Rule is April 21, 2005.

**Protected Health Information (PHI)** is any health information by which there is a reasonable basis to believe that an individual may be identified, and that relates to the past, present, or future physical or mental health condition of an individual; the provision of health care services; or the payment for health care. **Electronic Protected Health Information (ePHI)** is PHI created, received, stored or transmitted electronically.

The primary focus of the HIPAA Security Rule is to:

- Ensure integrity, confidentiality, and availability of ePHI.
- Protect ePHI against improper modification or destruction.
- Protect against unauthorized use or disclosure of ePHI.

The Security Rule covers all electronic media used to create, receive, store, or transmit ePHI, such as:

- Computer networks, servers, desktop computers, laptop computers, personal digital assistants (PDAs) and handheld computers.
- Magnetic tapes, disks, compact disks (CDs) and other means of storing electronic data, including the Internet and SIU’s Intranet.

The Security Rule requires the designation of a HIPAA Security Officer. The HIPAA Security Officer for SIU is the SIU P&S Chief Information Officer, who has the support of the department of SIU P&S Information Systems and the department of SIU SOM Information Resources in handling any HIPAA security issues. Departmental HIPAA Security Liaisons have also been identified who are responsible for ensuring that their department complies with all security policies and procedures, and provides the appropriate safeguards for protecting any and all departmental ePHI. Please check with your network administrators and/or desktop support personnel for your HIPAA Security Liaison contact. Education and compliance with the HIPAA Security Rule is a cooperative effort between all parties mentioned above, and all members of our workforce.

The Security Rule lists a wide range of activities for which SIU must provide protection. The rule **only** applies to protecting electronic protected health information (ePHI). For example, we must safeguard computer hardware and software with ePHI; buildings that house computer hardware and software with ePHI; storage and disposal of ePHI data and the back-up of ePHI data; and who has authorized access to ePHI data. **Electronic PHI may be in the form of a database, spreadsheet, document, folder, storage device, or any other form of electronic information.**

Electronic PHI is considered highly confidential. You should be aware of and/or apply the following safeguards in protecting ePHI:

- Log off or lock your computer (Ctrl-Alt-Del) when you will be away from your work area. All computers, PDAs, laptops, and other computer devices should be secured when not in use.
- Where possible, close and lock doors that allow access to ePHI and/or computer resources.
- Do not share your password with anyone, and never post your password.
- Only use passwords that are not easily guessed.
- No unauthorized software will be installed on devices accessing SIU ePHI. Any and all software must be approved by your HIPAA Security Liaison and/or the HIPAA Security Office.
- Email is not a secure medium and transmission of ePHI should be minimized. SIU P&S does not recommend the use of e-mail communication with patients. If a patient finds an individual provider's e-mail address, the provider needs to make it clear to patients that the use of e-mail is to be restricted to non-emergent situations, and that a prompt response is not always possible. SIU P&S does not recommend the discussion of health conditions via e-mail. The recommendation is to use a standard response such as: "Thank you for your inquiry, but I cannot respond via e-mail as it involves information that is confidential in nature. If you wish to discuss this matter further, please call us to make an appointment and I would be happy to answer your questions." Please refer to the SIU P&S Email Policy.
- Signing the SIU Statement of Confidentiality is a condition of employment at SIU.
- Only access patient information or protected health information when needed to perform your job.
- Access to confidential information and ePHI is only granted to authorized individuals on a need-to-know basis.
- Never disclose or provide ePHI to others except in accordance with SIU policies and procedures.
- Never bypass or disable anti-virus software on SIU computers and devices.
- The HIPAA Security Office must be notified if you transfer departments or terminate employment.
- Do not use computers to engage in any activity that is in violation of SIU policy, or that is illegal.
- Unlawful or unauthorized access, use, or disclosure of confidential information is prohibited.

**All SIU HIPAA Security Policies & Procedures, and the above safeguards apply to all SIU and non-SIU workstations and devices that access, store, or transmit ePHI, including home computers.**

The SIU P&S HIPAA Security Policies & Procedures may be found at the following link:  
**<http://intranet.siumed.edu/forms/pns/hipaa/>**.

If you are uncertain if ePHI is accessed, created, received, stored or transmitted electronically by you, or if you believe the appropriate safeguards are not in place to protect ePHI, then please contact your HIPAA Security Liaison or the HIPAA Security Office at 217.545.1257 or email us at **[siups\\_ssu@siumed.edu](mailto:siups_ssu@siumed.edu)**.

---

**Sandra A. Walters**  
Chief Information Officer  
Southern Illinois University School of Medicine  
SIU Physicians & Surgeons, Inc.  
PO Box 19631  
Springfield, IL 62794-9631  
217-545-7888 Office  
217-545-1755 Fax