April 18, 2005 (1st distribution)
January 6, 2006 (2nd distribution)
July 5, 2011 (3rd distribution)
May 31, 2012 (4th distribution)

MEMORANDUM

TO: SIU School of Medicine Faculty, Staff, & Students
FROM: Don Chenoweth CIO, SIU HealthCare
SUBJECT: HIPAA and HITECH 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 Rules from 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. In 2009 the American Recovery and Reinvestment Act was passed and the Health Information Technology for Economic and Clinical Health Act (HITECH) was included as part of the ARRA act. The HITECH act expanded on the enforcement, notification and rights to obtain a patient record.

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

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

- Computer networks, servers, desktop computers, laptop computers, iPads, personal digital assistants, etc.

- (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 HealthCMO, who has the support of the department of SIU HC IT and the department of SIU SOM IT 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 department administrator or Clinic manager 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 HITECH act addresses the following:

- Enforcement – the act included fines up to $250,000 for first offence and up to $1.5 Million for repeat offences.
- Notification – patients are required to be notified by law and if the exposure is over 500 patients then HHS is required to be notified.
- All patients have the right to a copy of their record and if the patient record is digital they have a right to a digital copy.

It should be noted that fines at the above level have been levied since the act was passed. In fact "A report from the accounting firm Kaufman , Rossin & Co. showed that in the first year since the HITECH Act was passed, about 5 million people had their personal health information compromised, either as a result of theft or because the data was lost. [1]

The Security Rule lists a wide range of activities for which SIU must provide protection. The rules originally applied to electronic PHI but the new rules in HITECH include paper documents as well. In any case 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 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.

[1] HIPAA privacy actions seen as warning, Computerworld February 25, 2011

- 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 not be done. The Centricity EHR at SIU HC has secure e-mail that should be used to communicate with patients. If you have questions please contact SIUHC IT for ways to communicate secure e-mail.**
- 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 HC 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.**

____

Don Chenoweth Chief Information Officer
Southern Illinois University School of Medicine and SIU HealthCare
PO Box 19631 Springfield, IL 62794-9631
217-545-7888 Office 217-545-1755 Fax