# HIPAA Security Rule

Your Responsibilities for Safeguarding Electronic Protected Health Information (ePHI)

## WHAT IS THE HIPAA SECURITY RULE?

HIPAA Rules continue past Privacy and into the area of Security. The HIPAA Security Rule is the latest portion of the larger Health Insurance Portability and Accountability Act (HIPAA). It is time to prepare for compliance with this Security Rule as it becomes effective **April 20, 2005**.

The purpose of this brochure is to raise awareness and educate you about your role and responsibilities for keeping electronic protected health information (**ePHI**) safe from unauthorized use, disclosure or corruption. You must be aware of and follow these minimum safeguards:

**1. Passwords:** Passwords protect against someone entering or completing transactions in your name from your account (e.g., entering orders or sending e-mail). Your user name and password is a unique identifier to you only. You are solely responsible for any misuse of your account. A secure password is one that is not found in the dictionary and has a minimum length of 6 characters with at least one upper case alpha, one number, and one special character (e.g. J2, nr!).

**2. Logoff or Lock:** Limit exposure of computer screens and applications containing ePHI by **never** leaving a computer or workstation unattended unless you have logged off or locked the computer. Failure to lock or logoff your computer when you walk away leaves your legal documentation open to alteration or other malicious activity under your name.

**3. Activity Monitoring and Review:** Scripps' systems are reviewed for logon and application activity to evaluate appropriateness of access to the network and to specific patient accounts. Inappropriate access to patient data (e.g., patients not in your care) will result in medical staff sanctions. If you have reason to believe that your password may have been compromised or that someone is accessing your account, call the IS Help Desk (858-678-7500) or contact the Scripps Compliance Alertline (888-424-2387). Change your password immediately.

**4. Suspicious Activity:** Any computer that is not performing as expected, is suspected of having a virus or other malicious software, or appears to have been used for unauthorized activity on Scripps' network should be reported to the IS Help Desk. If you use remote access to connect to Scripps' network, you must ensure that your home or office computer has active and current anti-virus software, that all security patches are applied, and any other precautions outlined in your access agreement are being followed. Report missing, lost or stolen devices immediately to the IS Help Desk.

**5. E-mail:** You need to know that your e-mail communications are not secure unless specifically protected. Standard e-mail is not encrypted and is not secure because: 1) it can be altered and/or forwarded, 2) it can be "spoofed" or made to look like it came from someone other than the actual sender, and 3) if forwarded or auto-forwarded to an e-mail address outside Scripps (e-mail address that does not end in "@scrippshealth.org"), it is transmitted in clear text. Because of the potentially insecure nature of electronic communications, it is Scripps policy that any communication containing ePHI should

be limited to the minimum amount of information necessary. If possible use a method of communication other than e-mail. If a method of communication other than e-mail cannot be used, you are responsible to know and follow institutional policies and procedures for protecting and, in some cases, obtaining authorization for the e-mail. Contact the IS Help Desk or Health Information for specific direction.

**6. Storing and Transmitting Information: PHI should not be stored on local hard drives or removable devices** such as laptops, floppy disks, backup tapes, CD-ROMs, zip or USB flash drives. ePHI is the property of Scripps Health and may not be removed or transmitted from Scripps facilities except in accordance with institutional policies and procedures. ePHI will **not** be stored on non-Scripps owned or controlled removable devices. Whenever possible apply encryption and password protection on removable devices. Report missing, lost or stolen removable devices to the Help Desk immediately.

**7. Protecting Your Computer:** Ensure your computer is updated with the latest anti-virus software and Windows operating system updates. Out-of-date anti-virus or operating system software may compromise your computer and networks to which your computer is connected. Such compromises may result in inappropriate PHI disclosure.

## IF YOU LOG ON TO THE SCRIPPS HEALTH NETWORK OR ANY COMPUTER SOFTWARE APPLICATION, YOU MUST:

**1.** Protect and don't share your logon ID and password. Know how to create a secure password.

**2.** Logoff or Lock your workstation. Never leave a workstation unattended and unlocked when you are logged in. An unauthorized transaction could occur using your electronic identity.

**3.** Access only accounts of patients who are under your care. HIPAA requires that application activity and network access be monitored and reviewed on a regular basis.

**4.** Notify the Information Services Help Desk (858-678-7500) of suspicious activity on or around workstations, missing, lost or stolen computer equipment or malfunctioning computer devices, unauthorized software installed on a workstation, and potentially malicious software (viruses).

**5.** Protect all e-mail with PHI that is sent to external parties by using encryption or other methods to protect e-mail contents. Keep in mind E-mail is not a secure form of communication.

**6.** Avoid storing electronic protected health information on hard drives or removable devices, (e.g., memory sticks, PDAs, laptops) on non-Scripps owned or controlled devices. Encrypt temporary files and delete when finished.

### Additional Resources:

San Diego Regional HIPAA Readiness Council
http://sdhipaa.org
Physician community generic access;
**username:** HIPAA; **password:** READY

San Diego County Medical Society
http://www.sdcms.org/

California Office of HIPAA Implementation
http://www.ohi.ca.gov/state/calohi/ohiHome.jsp

Dept of Health and Human Services Offices for Civil Rights (OCR)
http://www.hhs.gov/ocr/hipaa/

**HIPAA Security Awareness Program**

*This pamphlet was prepared by the San Diego HIPAA Consortium and contains important information to help you satisfy the federal security regulations for information security training. Please share this document with your colleagues and staff.*

*8655-941SW 4/05*