GENERAL COUNSEL NOTE

2008

As of April 21, 2005, all healthcare providers including Vanderbilt University Medical Center (VUMC) are required to be compliant with the Health Insurance Portability and Accountability Act (HIPAA) security regulations (the Security Rule). Recent accounts of security breaches and stolen laptops containing patient information highlight the need for all clinicians to learn about and apply security rule requirements to their practices. This General Counsel Note summarizes the key provisions of the Security Rule and offers compliance tips for busy VUMC clinicians.

Why is the HIPAA Security Rule needed?

- To protect Vanderbilt's electronic protected health information (EPHI) from accidental or intentional destruction, alteration or loss. The integrity and availability of individually identifiable patient health information that is created, received, maintained or transmitted by VUMC must be maintained so that it can be used by VUMC clinicians to provide high quality care to patients.
- To protect against any reasonably foreseeable threats or hazards to the security or integrity of EPHI, such as hackers interested in stealing patient data for personal gain.
- To protect against reasonably anticipated accidental/inappropriate disclosures of EPHI that could result in patient data accidentally falling into the wrong hands.

What is EPHI?

EPHI is protected health information created, received, maintained, or transmitted electronically. Protected health information is confidential patient information that identifies a patient, including data such as name, birth date, telephone/fax numbers, street address, Social Security number, e-mail address, insurance plan number, medical record number, and photos/videos.

Why do we have both a Privacy Rule and a Security Rule?

The subject of the HIPAA Privacy Rule is the "what." It gives patients the right to have their confidential patient information protected from unauthorized use or disclosure. The Security Rule deals with the "how." Security regulations require administrative, physical, and technical safeguards to protect patient privacy.

What do I need to do?

1. **Protect your password:** You are responsible for all activity conducted using your user ID and password. Do not share your user ID and password with any other person and change your password regularly. Do not login to any system using your user ID and password and then allow someone else to work in that system under your password.

2. **Secure your workstation:** Do not leave a computer unattended while you are logged on. Always log off applications containing confidential information or EPHI when you are finished. Lock the computer workstation if you must walk away before you are finished. Leave EPHI in secure network servers whenever possible. Remove media containing EPHI from a computer that you are not using and keep it under lock and key. Keep laptops, PDAs, CDs, thumb drives and other mobile media containing EPHI under lock and key.

3. **Mobile computer precautions:** If an authorized Vanderbilt purpose exists for you to store EPHI somewhere other than a VUMC network server, then you are accountable for the protection and security of the EPHI consistent with the Security Rule of HIPAA. Mobile devices have increased vulnerability to loss and theft and EPHI accessed and stored on mobile devices require increased levels of protection, up to and including:

    a. Password protection on the device;
    b. Use of minimum necessary information to accomplish the Vanderbilt purpose (such as avoiding the use of patient names as an identifier in conjunction with the patient's full social security number, medical record number, or other direct identifiers);
    c. Keep the device locked when not in use; and
    d. Encryption of the EPHI stored on the device.

4. **Safeguard EPHI on home computers:** Keep remote authentication codes confidential. Do not allow family members and other unauthorized persons to use computer equipment provided by Vanderbilt for work performed at home. Take precautions so that family members and other unauthorized persons are not able to view confidential information that appears on the screen when using the system. Be sure to have current versions of anti-virus software and a firewall on any home computer used to access, store, or transmit EPHI.

5. **Viruses:** Do not open email with attachments or with odd subject headings from unknown senders. Do not download software from the Internet or that has not been verified as safe.

Report privacy/security concerns: Report any potential privacy or security violation of as soon as it is discovered to the VUMC Privacy Office at 936-3594 or the VUMC Help Desk at 343-4357. Theft of a mobile device containing EPHI must also be reported to the Vanderbilt Police Department or local law enforcement in the community where the theft is believed to have occurred.

This Note is for informational and educational purposes only.
It states general propositions and is not intended to
and should not be viewed as legal advice from
the Office of the General Counsel.