What is HIPAA?

HIPAA (Health Insurance Portability and Accountability Act of 1996) is a federal statute that publishes security standards for healthcare organizations. These organizations are mandated under this federal law to meet minimum standards of due care to provide confidentiality and protection for patient physical and individually identifiable electronic Protected Health Information (e-PHI).

Why?

San Jose State University is committed to privacy and security. Protection of sensitive electronic health information is the duty and mission of the University, and individuals handling this information play a critical role in helping not only improve security, but help safeguard sensitive electronic medical records. The University has a history of leadership in establishing improvements in privacy and security of sensitive information for universities. Finally, San Jose State University is mandated by federal law to comply with HIPAA security standards under Title II to provide privacy and security for the protection of physical and electronic Individually Identifiable Health Information in the University health service centers. When HIPAA rules are violated, individuals can face civil penalties of $100 to $50,000 per violation and up to $1.5 million per year. In addition, criminal penalties may also be enforced under HIPAA, including imprisonment. HIPAA violations in excess of 500 total records must be reported to local media.

Finer Points

HIPAA is composed of both a privacy and a security rule. The HIPAA Privacy Rule creates national standards for protection of individual medical records and other personal health information. It sets rules for the use and disclosure of patient's medical information, and gives these patients rights' over their health information. HIPAA rules also specify the definition of organizations that must comply with HIPAA rules requirements. These organizations include "covered entities" and "business associates." HIPAA covered entities include "Health Care Providers", such as SJSU health service centers. Under the HIPAA Security Rule, covered entities must comply with specific technical and physical safeguards for protection of the confidentiality, integrity, and availability of processed electronic health information. Finally, HIPAA also specifies a Breach Notification Rule, which defines how covered entities and their business associates must provide notification following a breach of unsecured protected health information.

What you need to know

At San Jose State University, individuals that handle HIPAA information play a key role in helping to safeguard the privacy of private health information. It is the responsibility of everyone involved to help protect this information. Being proactive with security in mind can help prevent HIPAA security related incidents from arising.

- SJSU must comply with HIPAA security rules, for the protection of HIPAA information processed in the Student Health Center and Speech Therapy Clinic.

- **Limit use and disclosure of PHI (Protected Health Information):** Employees should take measures to limit the use and disclosure of PHI to the minimum necessary in order to meet the health services functional requirement.
- **Protect stored PHI in electronic format:** For any computers processing HIPAA information, HIPAA information must be stored encrypted. Processing electronic PHI should be stored on network shares / drives, to protect this data. Limit the use of PHI in emails, and delete emails containing PHI.
- **Protect computers with Security Best Practices in Mind:** For any computers processing HIPAA information, keep in mind some security best practices:
    - **Robust passwords:** Follow robust password guidelines outlined by the university. Never share or disclose your password to a 3rd party.
    - **Malicious Emails and Attachments:** Follow common sense and avoid clicking on suspicious links and opening suspicious attachments via email.
    - **Use Anti-Virus program:** Ensure to keep Anti-Virus programs up to date, active, and periodically scanning your computer for malicious software and attachments.
- University HIPAA information is classified as Level 1 information, and must meet University security requirements for protection of Level 1 information. For more information on the requirements for encryption and handling of HIPAA information, refer to the SJSU "Information Classification and Handling" security standard [2].
- **HIPAA Breach Notification:** If you suspect a potential unauthorized disclosure of HIPAA information, contact the Information Security Office.

More Information

[1] U.S. Department of Health and Human Resources Health Information Privacy (external link) http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

[2] San Jose State University: "Security Standard for Information Classification and Handling"