**AS—05 Security Awareness and Training**

**Purpose**

To develop a security awareness and training program for all members of its workforce (including management).164.308(a)(5)(i)

**Guidance**

Regardless of the Administrative Safeguards a covered entity implements, those safeguards will not protect the ePHI if the workforce is unaware of its role in adhering to and enforcing them. Many security risks and vulnerabilities within covered entities are internal. This is why the next standard, Security Awareness and Training, is so important. In addition, periodic retraining should be given whenever environmental or operational changes affect the security of ePHI. Changes may include new or updated policies and procedures; new or upgraded software or hardware; new security technology; or even changes in the Security Rule.

**Security Reminders**

Implementation: To develop processes and procedures for periodic security updates. 164.308(a)(5)(ii)(A)

* Establish security awareness and HIPAA training for all members of the UCSC workforce who are involved in the creation, transmission, and storage of ePHI. Training activities include:
	+ Initial security awareness and HIPAA training for individuals with ePHI-related job duties. Training will include UCSC Password Standards and the importance of protecting against malicious software and exploitation of vulnerabilities.
	+ Review of changes to internal policies, procedures, and technologies
	+ Periodic reminders about security awareness and HIPAA
	+ Security notices or updates regarding current threats
* HIPAA entities must maintain records of training materials and completion of training for six years.

**Protection from Malicious Software**

Implementation: Develop procedures for guarding against, detecting, and reporting malicious software. 164.308(a)(5)(ii)(B)

To protect all devices against malicious software, such as computer viruses, Trojan horses, spyware, etc., implement the following. Also ensure the safeguards and configurations below are included in the standard set-up procedures for new systems and workstations that contain or access ePHI.

* Run versions of operating system and application software for which security patches are made available and installed in a timely manner.
* Harden systems. “Hardening” includes:
	+ Install OS and third party application updates (patches) and keep them current
	+ Change or remove default logins/passwords
	+ Disable unnecessary services
	+ Install virus and malware protection software and update them at least weekly
	+ Set proper file/directory ownership/permissions; NTFS should be used on Windows servers and shared workstations
* Periodically, and at least annually, review HIPAA workstation browser settings to ensure that they comply with the recommended browser security settings: <https://www.us-cert.gov/publications/securing-your-web-browser#how_to_secure>.
* Periodically, and at least annually, review email client settings to ensure they comply with current ITS recommendations for email client settings: <http://louisville.edu/email/cardmail-faqs>
* Perform periodic network vulnerability scans of systems containing known ePHI, and workstations that access ePHI, and take adequate steps to correct discovered vulnerabilities.
* Implement e-mail malicious code filtering.
* Install/enable desktop firewalls (hardware and/or software) to reduce threat of unauthorized remote access.
* Intrusion detection software and/or systems may also be installed to detect threat of unauthorized remote access.

**Login monitoring**

Implementation: To develop procedures for monitoring login attempts and reporting discrepancies. **164.308(a)(5)(ii)(C)**

* Implement policies and procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports
* Regularly review information system activity and log-in attempts
	+ Log Procedures
		- Enabled at the OS, application/database and system/workstation level
			* Failed and successful logins
			* Modification of security settings
			* Privileged use or escalation of privileges
			* System events
			* Modification of system-level objects
			* Session activity
			* Account management activities including password changes
			* Policy change
			* Workstation firewalls
			* Anti-virus/anti-malware product
			* Applications such as web servers
		- Captured information for the above items as feasible
			* Date and time of activity
			* IP address for connection logs
			* Identification of user performing the activity
			* Description of attempted or completed activity
			* Application logs:
				+ Client requests and server responses
				+ Abnormal usage (number of transactions, usage spikes, etc.)
				+ Abnormal application behavior (repeated restarts)
				+ Data modification – if regulation or law required
		- Reviewed in response to suspected or reported security incidents on ePHI system or per IT direction
		- Reviewed in response to suspicious activity, escalated as required
		- Individuals may not be the sole reviewer of their own activity
		- System owners are responsible for determining systems reviewed
* Maintain documentation of periodic log reviews
* Logs relevant to security incidents should be retained for \_\_\_ years and other log data for a minimum of \_\_\_\_ days or as per university policy, practice or law/regulation
* Logs must be secured and protected

**Password management**

Implementation: To develop procedures for creating, changing, and safeguarding passwords. **164.308(a)(5)(ii)(D)**

* Passwords for systems containing or accessing ePHI will comply with the UofL Password Strength and Security Standards:

<https://sharepoint.louisville.edu/sites/policies/library/SitePages/Information%20Technology/Passwords.aspx>

* Enforce UofL password complexity requirements for third-party access were possible.