UNIVERSITY OF CENTRAL FLORIDA

University Standards

Subject:	HIPAA Infrastructure Requirements
Standards Number:	106
Effective Date:	12/11/2019
Revised Date:	
Responsible Authority:	Information Security Office
Pages:	6

ACCOUNTABILITY/APPLICABILITY:

These standards apply to all University of Central Florida owned infrastructure connected to the university network via physical, wireless, VPN connections, hosted with a cloud vendor and contains protected health information (PHI). These standards should provide UCF System Administrators an understanding on what security configurations should be applied to university infrastructure in order to bring them into compliance with HIPAA standards.

STANDARDS STATEMENT:

The purpose of this document is to establish minimum-security standards that should be applied to all university infrastructure that contains protected health information (PHI) in order to maintain the confidentiality, integrity, and availability of university information systems.

Any exception to the standards must be documented and approved by a designated HIPAA Security Officer in advance.

STANDARDS:

Encryption in transit

- **SSL Certificates & HTTPS (SHA 256 or greater)** – All types of web-based or client access to a patient's PHI are encrypted and secure to prevent unauthorized connections. **Encryption** is required on all integrations between UCF systems or with third parties. These integrations should use secure encrypted protocols such as SFTP, HTTPS, etc., or the use of a VPN for integrations as needed.

Encryption at rest

- **AES Encryption (or strongest level of encryption supported by application)** – Advanced Encryption Standard used to encrypt PHI stored on dedicated servers and databases
    - Encryption and Decryption – 164.312(a)(2)(iv): Implement a method to encrypt and decrypt electronic protected health information.

      Encryption – 164.312(e)(2)(ii): Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. Other types of encryption may be acceptable if more modern encryption algorithms are unsupported
- **Disk Encryption –** Disk encryption on all underlying ePHI storage, e.g. disks where databases are stored, file servers, etc.

Logging

- **OS and Network Audit Logging** - Audit logs must be enabled on all appropriate network devices and operating systems to track when users are accessing or attempting to access systems. *Retention period of one year.*
- **Application Audit Logging** – Audit logs must be enabled on applications to maintain chain of custody, including:
    - Who accessed the data
    - When the data was accessed and for how long
    - What data was accessed
    - What changes were made to the data
    - Retention period of seven years
- **Database Security Logging** – Database security logs must be enabled to record who accessed the data and when. *Retention period of one year.*
- **Central Logging Policy –** All logs should be forwarded to the dedicated HIPAA environment in the enterprise Security Incident and Event Management (SIEM) tool.

- **Data retention** - Per Florida Statute 64B8-10.002(3), FAC : A licensed physician shall keep adequate written medical records, as required by Section 458.331(1)(m), Florida Statutes, for a period of at least **five years** from the last patient contact; however, medical malpractice law requires records to be kept for at least **seven years**. [5 & 6]

- **Log and Access Review** Per HIPAA Rule § 164.308(a)(1)(ii)(D): *Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports*.

  - The HIPAA security officer or designee responsible for the HIPAA system and data in question should develop processes to request and review the relevant logs for their systems on a regular basis, such as monthly, quarterly or as needed.

  - To meet this requirement, it is recommended to utilize an applications reporting capabilities and to export relevant logs to the enterprise SIEM. Contact the Security Operations Center team (soc@ucf.edu) for assistance with sending relevant logs to the Enterprise SIEM. SOC provides the SIEM infrastructure and support ingesting log sources, and functional units are responsible for regular monitoring and reporting incidents to SIRT.

Network Access Controls

- **Firewall Services** – A secure firewall must be deployed to prevent unauthorized access to protected infrastructure.

- **Remote VPN Access** – In cases where limited application encryption is available, those with proper access should be able to access the application data using a remote computer. Additional restrictions may be applied to prevent remote access.

- **Internal/Private Network Standards**
  - Application and data workloads must be placed in a “Zone 1” network with micro-segmentation, internet egress filtering and default inbound network filtering

  - Administrative access to “Zone 1” systems must be done via MFA-enabled jump box

  - Micro-segmentation within this "Zone 1” systems only allows specific servers and clients to communicate over specified ports

- **Public facing network standards**

  - Placement of public facing workloads in a “Zone 4” DMZ network with micro-segmentation, internet egress filtering, and default outbound (to all other networks and IPs) denies applied
  - Administrative access to “Zone 1” networks must be done via MFA-enabled jump box.
  - Generally, this would be secured in line with Zone 1 standards (strict whitelists to IP's or well-defined ranges)
  - Public workloads should be placed behind a load balancer and web application firewall

- **Multi-factor Authentication -** MFA must be enabled for all server-level access. MFA is preferred and recommended for application access

- **Disaster Recovery** – A documented backup and recovery plan in case of lost PHI or server malfunction

- **Annual HIPAA Training (COM HIPAA Training) -** for any IT support person accessing any applications and servers housing HIPAA data

SQL Database Standards

- **Database-level encryption -** Transparent Data Encryption (TDE) enabled on all SQL databases.
- **Instance segregation -** Dedicated database instance in "Zone 1" network for ePHI data. Do not mix Highly Restricted data with Restricted data on same SQL instance.
- **Encryption in transit -** Certificates applied to all SQL database instances.

Security Incident Response Procedures

- In cases of a suspected security incident, staff must contact UCF's Security Incident Response Team sirt@ucf.edu.

Vulnerability Scanning

- Perform vulnerability scans on a monthly basis.
- Conduct vulnerability scans when systems are deployed using a "HIPAA Compliance Scan" policy.

Rules for Cloud Hosting

- BAA must be present with cloud hosted HIPAA data. BAAs are in place with AWS and Azure.

Access Approval

- Approval of the HIPAA security officer (or designee) responsible for the HIPAA system and data in question is required for access to HIPAA data.

Physical Security

- UCF-hosted HIPAA infrastructure must reside in UCF's Azure[8] cloud, UCF's colocation facility – Data Site Orlando[7], or the Health Sciences Data Center that meet HIPAA physical security standards.

DEFINITIONS:

HIPAA. The Health Insurance Portability and Accountability Act of 1996. HIPAA protects the security of individually identifiable health information.

Data Site Orlando (DSO). UCF's colocation facility in Orlando, FL hosting infrastructure and information. This data center aligns with UCF and industry guidelines/standards for restricted and/or highly-restricted data.

SIEM. Security Information and Event Management. A security tool that provides real-time monitoring, correlation of events, and notifications.

REFERENCES:

1. https://www.healthit.gov/providers-professionals/security-risk-assessment-tool
2. http://scap.nist.gov/hipaa/
3. https://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html
4. https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html
5. https://www.hipaajournal.com/hipaa-retention-requirements/
6. https://flboardofmedicine.gov/help-center/how-long-must-a-healthcare-practitioner-maintain-a-patient%C2%80%C2%99s-records/
7. https://www.datasitecolo.com/products-services/security-compliance/
8. https://docs.microsoft.com/en-us/azure/security/azure-physical-security
9. https://www.microsoft.com/en-us/trustcenter/Compliance/hipaa
10. https://www.atlantic.net/hipaa-data-centers/hipaa-compliant-it-infrastructure-guide/

CONTACTS:

Information Security Office https://infosec.ucf.edu infosec@ucf.edu	Security Incident Response Team (SIRT) https://infosec.ucf.edu/incident-response/ sirt@ucf.edu
Identity Access Management (IAM) https://infosec.ucf.edu/iam iam@ucf.edu	UCF IT Support Center (407) 823-5117 https://ucf.service-now.com/ucfit itsupport@ucf.edu
Security Operations Center (SOC) soc@ucf.edu	

Revision Date	**Summary of Change**

INITIATING OFFICE: Information Security Office

STANDARDS APPROVAL
(For use by the Information Security Office)

Standards Number: *106*

Initiating Office: [Information Security Office]

Chief Information Security Officer: *Chris Vakhordjian*

Signature: chrisv chrisv
dc=edu, dc=ucf, dc=net, ou=People, cn=chrisv,
email=Chris.Vakhordjian@ucf.edu
2020.03.10 16:16:14 -04'00' Date: ____________