NORTHWESTERN
UNIVERSITY

HIPAA/ISO INFORMATION SECURITY GUIDANCE

Foreword

This Security Guidance describes the Standards and Implementation Specifications required by the Health Information Portability and Accountability Act (HIPAA) and corresponding controls of Information Standards Organization's (ISO) Security Standards (27001/2). HIPAA requires compliance with Administrative Safeguards 164.308, Physical Safeguards 164.310, and Technical Safeguards 164.312. In response, the University adopted the ISO standards and created this guidance to identify the actions that, when executed, help to meet the HIPAA/ISO requirements.

This document is organized by sections (Administrative, Physical and Technical Safeguards) and identifies:

1. The Standards and Implementation Specifications described within HIPAA;
2. The corresponding ISO standard and actions; and
3. References to Northwestern's Information and Systems Security Plan/Procedures (ISSP/P) (see: http:/www.it.northwestern.edu/bin/docs/ISSPP.pdf).

Implementation Specifications consist of Actions that are either:

1. Required - must implement the specification
2. Addressable - implement the specification if reasonable and appropriate, or implement an equivalent alternative.

References to the ISO Standards and ISSP/P are offered as the basis for the Required or Addressable Actions and provide support and justification of the Actions.

Additional Information

This document is owned by Northwestern University's Information and Systems Security/Compliance, subject to periodic review and updates.

Please refer any questions to the University HelpDesk (847-491-HELP) or email security @northwestern.edu.

Change History

Date	Ver.	Author/Contact Information	Comments
08 Aug 2014	1.0	D. Kovarik david-kovarik@northwestern.edu Office: (847) 467-5930	Initial publication of document
20 Nov 2014	1.1	D. Kovarik david-kovarik@northwestern.edu Office: (847) 467-5930	Provide corrected link to reference this document

HIPAA/ISO Information Security Guidance

I. ADMINISTRATIVE SAFEGUARDS 164.308

Administrative Safeguards are administrative actions, policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect electronic protected health information (ePHI) and to manage the conduct of the entity's workforce in relation to the protection of that information.

Security Management Process 164.308(a)(1)

I. A. Risk Analysis

"Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity."

Required Actions:

Identify and **document** any of your data subject to regulatory or compliance requirements (i.e. sensitive data).
Determine if any existing or new processes require the handling of sensitive data; document any results.
Determine if existing or new processes are capable of adequately protecting the confidentiality, integrity, and availability of sensitive data; document any results. **Evaluate** the potential vulnerabilities of said processes.
Determine and **document** the consequences if a vulnerability were exploited, i.e. potential cost to your organization in the event that sensitive data is disclosed or exposed without permission.

☐ **Reference:**

ISO 27002 - 4.1 Assessing Security Risks
NUIT ISSP/P - 10.1 Information Security Risk identification and 10.2 Information Systems Security Risk Analysis/Ranking

II. B. Risk Management

"Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a) – Security Standards."

Required Actions:

Identify instances where risk to sensitive data could be eliminated, reduced, transferred, or accepted.
Implement controls that are required by regulations. Should any implementation not be feasible, **identify** and **deploy** compensating controls; document the decision and any supporting arguments.
Attempt to strike a balance between the cost of implementing controls and the cost to the organization, should a data loss or exposure occur.
Document all decisions and supporting arguments where there is a departure from required implementations and controls.

☐ **Reference:**

ISO 27002 - 4.2 Treating Security Risks
NUIT ISSP/P - 10.0 Information Systems Security Risk Management

III. C. Sanction Policy

"Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity."

Required Actions:

Document any activity that contributed to a suspected or actual condition of noncompliance.
Confirm any conditions of noncompliance. Contact NUIT Information and Systems Security/Compliance for assistance.
Contact Human Resources if a violation is confirmed.

☐ **Reference:**

ISO 27002-8.2.3 - Disciplinary Process
NUIT ISSP/P 7.3 – Sanctions

IV. D. Information Security Activity Review

"Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."

Required Actions:

Implement system logging to record the following:

- User Information: NetID, date and time of event
- Resource Information: Resource (e.g., file accessed, program or file executed), access type (e.g. read, write, create, delete), use of privileged commands or accounts, modification of user access or privileges, successful and unsuccessful access and/or execution
- System Information: change to system or security settings, successful and attempted access and/or execution

Store logs separately and restrict access to prevent tampering (e.g., write or copy log files to secure storage).
Institute a monitoring/review process of logs:

- **Determine** frequency based on risk (e.g., high risk recommends more frequent review)
- **Assign** responsibility for monitoring/review to appropriate personnel
- **Document** review process and evidence of its execution (e.g., log initialed by reviewer)

☐ **Reference:**

ISO 27002 - 10.10.2 Monitoring System Use
NUIT ISSP/P 10.2.1 Information Systems Security Activity Reviews

II. Assigned Security Responsibilities 164.308(a)(2)

Assigned Security Responsibilities

"Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart [the Security Rule] for the entity."

Required Actions:

Identify the data custodians(s) for the system(s) that you use to serve as:

- A guide in the implementation and enforcement of required security controls
- A liaison to data custodians
- A point of contact in the event of a suspected or known breach

Identify the systems that process and/or store sensitive data.
Define and document appropriate authorization and access levels.
Ensure all system users are informed of and acknowledge (in writing) the presence of sensitive data

☐ **Reference:**

ISO 27002 - 6.1.3 Allocation of Information Security Responsibilities
NUIT ISSP/P - 2.0 Northwestern University Information Security Responsibilities

III. Workforce Security 164.308(a)(3)

V. A. Authorization and/or Supervision

"Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed."

Addressable Actions:

Provide system users (new and existing) with a documented description of their job responsibilities (e.g. position description, statement of work, memorandum of understanding)
Before permitting access to systems, **inform** individuals of their obligation to:

- Comply with NU policies and applicable regulatory requirements.
- Preserve the confidentiality, integrity, and availability of assets.
- Report any suspected or actual security risk or breach according to established protocols.

☐ **Reference:**

ISO 27002 - 8.1.1 Roles and Responsibilities
NUIT ISSP/P - 2.0 Northwestern University Information Security Responsibilities and 3.2 Data Access Control/Management

VI. B. Workforce Clearance Procedure

"Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate."

Addressable Actions:

Contact Human Resources in all instances where an individual may have access to ePHI to determine the applicability of a background check; instances include, but are not limited to:

- Hiring of a new employee.
- Acquiring temporary or contract assistance.
- Transferring of employee into the department.
- Redefining roles/responsibilities that may result in access.
- Introduction of a new system or change to an existing system, providing access to ePHI.

☐ **Reference:**

ISO 27002 - 8.1.2 Screening
NUIT ISSP/P - 3.2.1.1 Eligibility for Information Access

VII.C. Termination Procedures

"Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends…"

Addressable Actions:

Reduce or remove access to sensitive data and facilities as soon as feasible and appropriate, and notify department management and Human Resources. **Consult** HR's Employment Termination Checklist.

For resignations, transfers and other instances where the separation is under amicable terms (e.g., contract expiration):

- **Consider** monitoring access until employment or contract service expires
- **Reduce** access to only those resources and facilities required to fulfill any remaining obligations or work activities through the stated end date;
- **Remove** all access to sensitive data and facilities as of the end date.

Where **termination is for cause**: remove access to all resources and facilities as soon as possible.

☐ **Reference:**

ISO 27002 - 8.3.1 Termination Responsibilities; 8.3.2 Return of Assets and 8.3.3 Removal of Access Rights
NUIT ISSP/P - 7.2 Terminations and Transfers

IV. Information Access Management 164.308(a)(4)

VIII. A. Isolating Healthcare Clearinghouse Function

"If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization."

Required Actions:

Establish and document, for all Users, an access policy that:

- Informs that the facility and system processes and/or stores ePHI;
- Requires Users acknowledge (in writing) the presence of, and their responsibility for protection of ePHI;
- Mandates all ePHI be handled securely;
- Requires approval of the system owner before system access is permitted;
- Permits access to the facility, system and data only where required;
- Describes appropriate conditions for disclosure of data;
- Requires periodic review of accesses to ensure proper authorization; and
- Notifies management in the event of a suspected or actual unauthorized exposure of ePHI.

☐ **Reference:**

ISO 27002 - 11.1.1 Access Control Policy
NUIT ISSP/P - 3.2 Data Access Control/Management

IX. B. Access Authorization

"Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism."

Addressable Actions:

Ensure assignment of an UserID that is unique to each individual (i.e., group IDs are not permitted access to ePHI);
Notify users in writing of their individual accountability for all activities occurring under the UserID and obtain their written acknowledgement;
Obtain approval of the user's management and the system owner before system and ePHI access is provided to the user;
Ensure that all users receive and acknowledge (in writing) appropriate training on the handling of ePHI, before access is permitted;
Permit users with access to systems and data on a "need-to-use" basis that aligns with assigned roles and responsibilities;
Identify, document, control and monitor UserIDs that are enabled to execute privileged commands or execute in a privileged state (e.g., sysadmins, DBAs, operators, etc.); segregate functions by UserID (where possible);
Reaffirm authorization and assignment of privileges to UserIDs thus enabled.
Perform and document periodic reviews of access to ensure proper authorization, removing or reducing access in a timely manner.

☐ **Reference:**

ISO 27002 - 11.2.1 User Registration and 11.2.2 Privilege Management
NUIT ISSP/P - 3.2.1 Access Authorization

X. C. Access Establishment and Modification

"Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process."

Addressable Actions:

Review and document semiannually all UserIDs that are enabled to execute privileged commands or execute in a privileged state (e.g., sysadmins, DBAs, operators, etc.).
Review and document annually all UserIDs with access to the facility, system and/or sensitive data
Ensure that system output (e.g., displays, reports, file transfers, system feeds, data exchanges, etc.) and intended targets are required and appropriate.

☐ **Reference:**

ISO 27002 - 11.2.4 Review of User Access Rights and 11.6.1 Information Access Restriction
NUIT ISSP/P – 3.2.1.1 Eligibility for Information Access and 3.2.1.3 Changing Information Access Authorizations

V. Security Awareness Training 164.308(a)(5)

XI. A. Security Reminders

"Implement periodic security updates."

Addressable Actions:

Make known to all personnel the policies, procedures, regulations and security practice applicable to the facility, system and handling of ePHI. **Conduct and document** training sessions annually.

Review individual roles and responsibilities

Inform all personnel of potential or known conditions that may expose the facility or system to unauthorized access or release of data

Instruct all personnel on their responsibility to report any suspected or actual security risk or breach

☐ **Reference:**

ISO 27002 - 8.2.2 Information Security Awareness, Education & Training
NUIT ISSP/P 7.4 - Security Training and Awareness

XII.B. Protection from Malicious Software

"Implement procedures for guarding against, detecting, and reporting malicious software."

Addressable Actions:

Ensure that all computers used to access a system that processes and/or stores ePHI adhere to NU's policies and practices to protect against malware.

All operating systems updates and patches should be applied regularly, on an ongoing basis.

All machines should have installed and active University-approved endpoint protection (e.g., firewalls, encryption, anti-virus/malware, etc.)

All machines should retain settings that automatically schedules regular updates of OS, applications and virus/malware definitions.

☐ **Reference:**

ISO 27002 - 10.4.1 Controls against Malicious Code
NUIT ISSP/P - 5.5 Malware and 4.1 Standard Workstation Configuration and 3.3.2 Securing Data – Data Encryption

XIII. C. Log-In Monitoring

"Implement procedures for monitoring log-in attempts and reporting discrepancies."

Addressable Actions:

Implement system logging to record user, resource and system information
Store logs separately and restrict access to prevent tampering
Institute monitoring/review process of logs
Determine frequency of review, based on risk
Assign responsibility for monitoring/review to appropriate personnel

☐ **Reference:**

ISO 27002 - 10.10 Monitoring
NUIT ISSP/P - 5.11.2 Computer, System, or Network Monitoring

XIV. D. Password Management

"Implement procedures for creating, changing, and safeguarding passwords."

Addressable Actions:

Ensure users are made aware of/comply with NU's policies and practices on passwords.
Follow the documented NUIT password requirements, including periodic changing of passwords.

☐ **Reference:**

ISO 27002 - 11.2.3 User Password Management; 11.3.1 Password Use and 11.5.3 Password Management System
NUIT ISSP/P - 3.2.3.1 Password Construction Requirements and 3.2.3.2 Password Management

VI. Security Incident Procedures 164.308(a)(6)

XV.Response and Reporting

"Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes."

Required Actions:

Ensure that all users are made aware of the University's incident response protocol.
Issue and document an annual reminder to all users.

☐ **Reference:**

ISO 27002 - 13.1.1 Reporting Information Security Events
NUIT ISSP/P - 10.5 IT Security Incident Response and Reporting

VII. Contingency Plan 164.308(a)(7)

XVI. A. Data Backup Plan

"Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information."

Required Actions:

Ensure that all users are made aware of and comply with their unit's backup plan
Issue and document an annual reminder to all users.

☐ **Reference:**

ISO 27002 – 10.5 Backup
NUIT ISSP/P - 3.5 Data Backup and Recovery

XVII. B. Disaster Recovery Plan

"Establish (and implement as needed) procedures to restore any loss of data."

Required Actions:

Ensure your business unit has developed and maintains a business continuity plan using the Northwestern University Business Continuity Plan Template.

☐ **Reference:**

ISO 27002 - 14.1.4 Business Continuity Planning Framework
NUIT ISSP/P - 6.4 Disaster Recovery Planning and 6.4.1 Applications and Data Criticality Analysis

XVIII. C. Emergency Mode Operation Plan

"Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode."

Required Actions:

Develop, implement and maintain business continuity plans to restore and ensure availability of information following interruptions to critical business processes.

☐ **Reference:**

ISO 27002 – 14.1.4 Business Continuity Planning Framework
NUIT ISSP/P - 6.4 Disaster Recovery Planning and 6.4.1 Applications and Data Criticality Analysis

XIX. D. Testing and Revision Procedure

"Implement procedures for periodic testing and revision of contingency plans."

Addressable Actions:

Regularly **test and update** business continuity plans to ensure they are up-to-date and effective.
Document test results.

☐ **Reference:**

ISO 27002 - 14.1.5 Testing, Maintaining & Reassessing Business Continuity Plans
NUIT ISSP/P - 6.4.2 Evaluation of Contingency Plans and 6.4.3 Testing Contingency Plans

XX. E. Applications and Data Criticality Analysis

"Assess the relative criticality of specific applications and data in support of other contingency plan components."

Addressable Actions:

Establish a ranked list of data applications to represent the order in which the data center would be brought back up, based upon applications and data dependency and criticality analysis.

☐ **Reference:**

ISO 27002 – 14.1.2 – Business Continuity and Risk Assessment
NUIT ISSP/P - 6.4.1 – Applications and Data Criticality Analysis

VIII. Evaluation 164.308(a)(8)

Evaluation

"Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operations changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart [the Security Rule]."

Required Actions:

Review annually your operation, business practices and policies to help ensure a continued state of regulatory compliance.
Request assistance from the NU's ISS/C or Audit and Advisory Services in the performance of an independent review.
Document all activities and results.

☐ **Reference:**

ISO 27002 - 6.1.8 Independent Review of Information Security and 15.2 Compliance with Security Policies and Standards, and Technical Compliance
NUIT ISSP/P - 10.4.1 IS Self-Audits and Activity Reviews and 10.2 IS Security Risk Analysis/Ranking

IX. Business Associate Contracts and Other Arrangements 164.308(b)(1)

XXI. Written Contract or Other Arrangements

"Document the satisfactory assurances required by paragraph (b)(1) [the Business Associate Contracts and Other Arrangements] of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a) [the Organizational Requirements]."

Required Actions:

Ensure contract/service agreements are reviewed before execution by the Office of General Counsel.
Contact NU's Consulting and Project Office before execution in all instances where information technology services are solicited or contracted.
Review the Service Provider Security Assessment policy to determine applicability to your contract.

☐ **Reference:**

ISO 27002-6.2.3 - Addressing Security in Third Party Agreements
NUIT ISSP/P 3.0 – Protection of NU Information and 3.2.3.4 Authentication for Services Outside the University Environment

PHYSICAL SAFEGUARDS 164.310

Physical Safeguards are physical measures, policies and procedures to protect an entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusions.

X. Facility Access Controls 164.310(a)(1)

XXII. A. Contingency Operations

"Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency."

Addressable Actions:

Implement and maintain a business continuity plan to address information security requirements and identify priorities for testing and maintenance.

☐ **Reference:**

ISO 27002 - 14.1.4 Business Continuity Planning Framework
NUIT ISSP/P – 6.4 Disaster Recovery Planning

☐ B. Facility Security Plan

"Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft."

Addressable Actions:

Identify the physical security perimeters and implement measures required to protect personnel, equipment and premises
Control reception areas, visitors, loading docks (shipping/receiving), fire exits and utility spaces to prevent unauthorized access
Locate equipment to minimize access and physical damage.
Contact Facilities Management and/or NUIT's Cyber Infrastructure for assistance in planning different or enhanced services

☐

☐ **Reference:**

ISO 27002 – 9.1.1 Physical Security Perimeter, 9.1.6 Public Access, Delivery & Loading Areas, 9.2.1 Equipment Siting and Protection, 9.2. Supporting Utilities and 9.2.3 Cabling Security
NUIT ISSP/P – 6.0 Physical Security

XXIII. C. Access Control and Validation Procedures

"Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision."

Addressable Actions:

Limit the access to IS facilities where feasible by permitting entry through a single portal (i.e., main lobby or entry way), and the access to areas where ePHI is processed or stored only to those who require it.
Ensure that all visitors are adequately identified, escorted and/or monitored in IS facilities; with entry and departure times, escort, areas visited, and reason for visit recorded and retained for audit review.
Ensure that production system components (data, programs, libraries) are segregated from non-production, with appropriate change management and monitoring processes.

☐ **Reference:**

ISO 27002 - 9.1.2 Physical Entry Controls; 12.4.2 Protection of System Test Data and 12.4.3 Access Control to Program Source Code
NUIT ISSP/P - 6.1.1 Physical Access Control, 8.3 Configuration Change Control

XXIV. D. Maintenance Records

"Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors and locks)."

Addressable Actions:

Maintain equipment and facilities in accordance with the supplier's recommended service intervals and specifications.
Permit only trained and authorized personnel to perform equipment and facility maintenance.
Retain records of equipment problems and maintenance activities
Ensure ePHI is removed from equipment before allowing its removal for repair –or- ensure repair personnel are authorized to access ePHI.

☐ **Reference:**

ISO 27002 - 9.2.4 Equipment Maintenance
NUIT ISSP/P - 6.1.3 Facility Maintenance Records

XI. Workstation Use 164.310(b)

XXV. Workstation Use

"Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation."

Required Actions:

Ensure all personnel are familiar and comply with NU policies on appropriate use of resources.

☐ **Reference:**

ISO 27002 - 7.1.3 Acceptable Use of Assets
NUIT ISSP/P - 4.0 Acceptable Usage

XII. Workstation Security 164.310(c)

XXVI. Workstation Security

"Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users."

Required Actions:

Whenever the computer is unattended, require users to execute a password-protected screen saver that requires a password to regain access to the computer.
For multi-user stations, **require** individual sign-on before permitting access.
Terminate all active application sessions at end-of-day or when the computer will not be used for an extended period (e.g., more than a few hours).
Use locking mechanisms (e.g., cable locks) to protect portable computer equipment (e.g., laptops, external hard drives, etc.) from unauthorized removal.

☐ **Reference:**

ISO 27002 – 11.3.2 Unattended User Equipment
NUIT ISSP/P - 5.4 Computer and Network Security Requirements

XIII. Device and Media Controls 164.310(d)

XXVII. A. Disposal

"Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored."

Required Actions:

Ensure all equipment that is replaced, reassigned or retired is protected from unauthorized removal/access.
Ensure that all data has been removed and rendered unrecoverable or unreadable.
Dispose of all equipment and media securely.
Update the equipment inventory to reflect the disposition of the equipment.

☐ **Reference:**

ISO 27002 - 9.2.6 Secure Disposal or Re-use of Equipment and 10.7.2 Disposal of Media
NUIT ISSP/P - 3.6 Data Computing/Media Reuse/ Destruction

XXVIII. B. Media Re-Use

"Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use."

Required Actions:

When re-assigning equipment, **ensure** all data has been rendered unrecoverable or unreadable and all programs have been uninstalled (to avoid licensing issues) **before reassignment occurs.**
Update the equipment inventory to reflect the disposition of the equipment.

☐ **Reference:**

ISO 27002 - 9.2.6 Secure Disposal or Re-use of Equipment
NUIT ISSP/P - 3.6 Data Computing/Media Reuse/ Destruction

XXIX. C. Accountability

"Maintain a record of the movements of hardware and electronic media and any person responsible therefore."

Addressable Actions:

Assign ownership to and responsibility for computing equipment
Maintain an inventory of computing equipment indicating ownership and responsibility.
Identify computing equipment used in the processing of sensitive data.
Monitor movement of equipment to prevent its unauthorized removal, and ensure appropriate relocation and/or prompt return when movement is authorized.
Perform an annual audit of the above information, and retain the results for a period of two years for purposes of audit.

☐ **Reference:**

ISO 27002 - 7.1.2 Ownership of Assets; 9.2.7 Removal of Property and 10.7.1 Management of Removable Media
NUIT ISSP/P - 3.6 Data Computing/Media Reuse/ Destruction

XXX. D. Data Backup and Storage

"Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment."

Addressable Actions:

Identify the data that needs to be backed up.
Select and implement a data backup plan.
Encrypt sensitive data before downloading to removable/portable media or require use of media that is self-encrypting.
Where long-term storage is required, **review** the use of alternate media to ensure the data is recoverable in the future.
When the media is retired, **ensure** that sensitive data is rendered unrecoverable from removable/portable media through wiping of the data or destruction of the media.
Update inventory when media is added or retired.

☐ **Reference:**

ISO 27002-10.5.1 Information Back-up
NUIT ISSP/P - 3.5 Data Backup and Recovery

TECHNICAL SAFEGUARDS 164.312

Technical Safeguards means the entity's technology and the policy and procedures that protect electronic ePHI and control access to it.

XIV. Facility Access Controls 164.312(a)(1)

XXXI. A. Unique User Identification

"Assign a unique name and/or number for identifying and tracking user identity."

Required Actions:

Require all users to obtain and use a unique id (e.g., NetID).
Where multi-user workstations or equipment is in use, **require** users to sign-in with their **own identity** before using the system or accessing data.
Install only applications that require users to authenticate.

☐ **Reference:**

ISO 27002 - 11.5.2 User Identification & Authentication
NUIT ISSP/P - 3.2.2 Workforce Member Identification and 3.2.3 Workforce Member Authentication

XXXII. B. Emergency Access Procedure

"Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency."

Required Actions:

Identify individuals who require access to ePHI and any resources required.
Establish and document the roles & responsibilities that allow access to ePHI while ensuring an appropriate segregation of duties.
Document the processes for requesting, authorizing and terminating access to ePHI.
Perform an annual review of the access permitted to ePHI, document the results, and retain the results for a period of three years for purposes of audit.

☐ **Reference:**

ISO 27002 - 11.1.1 Access Control Policy
NUIT ISSP/P - 3.2 Data Access Control/Management

XXXIII. C. Automatic Logoff

"Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity."

Addressable Actions:

Ensure the system or application enforces a "time out" (e.g., the application or network session is suspended) after a defined period of inactivity. The time-out delay should appropriately reflect the risk (e.g., sensitive data and a public area pose higher risk, thus a shorter time-out delay is appropriate).

☐ **Reference:**

ISO 27002 - 11.5.5 Session Time-out
NUIT ISSP/P - 5.4.1.3 Inactivity Log-off

XXXIV. D. Encryption and Decryption

"Implement a mechanism to encrypt and decrypt electronic protected health information."

Addressable Actions:

Identify those instances where encryption schemes are appropriate for access control following the guidance on NU encryption solutions.

☐ **Reference:**

ISO 27002 - 12.3.1 Policy on the Use of Cryptographic Controls
NUIT ISSP/P - 3.3 Confidentiality/Privacy

XV. Audit Controls 164.312(b)

XXXV. Audit Controls

"Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."

Required Actions:

Require users to acknowledge that access to ePHI is subject to a high degree of monitoring and auditing.
Maintain logs of the following activities:

- Authorized activities
- Privileged activities
- Unauthorized access attempts
- System alerts or failures
- Changes or attempt to change system settings and controls.

Execute a periodic review of the logs, document the results, and retain the results for a period of three years for purposes of audit.

☐ **Reference:**

ISO 27002 - 10.10.2 Monitoring System Use
NUIT ISSP/P 5.11.2 Computer, System, or Network Monitoring

XVI. Integrity 164.312(c)(1)

XXXVI. Mechanism to Authenticate Electronic Protected Health Information

Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner."

Addressable Actions:

Utilize secure data transmission protocols in the exchange of data with outside parties (e.g., SFTP, site-to-site VPN, etc).
Encrypt all communications and/or data files where ePHI is sent across any network.
Communicate passwords, when required, out of band (i.e., encrypted data sent via email, password via telephone).

☐ **Reference:**

ISO 27002-10.8.4 Electronic Messaging and 12.2.2 Control of Internal Processing
NUIT ISSP/P - 3.3.3 Securing Communications and 3.4 Data Integrity

XVII. Person or Entity Authentication 164.312(d)

XXXVII. Person or Entity Authentication

"Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed."

Required Actions:

Require NetID authentication and individual sign-on before permitting access.
Utilize NU approved solutions for remote access authentication.

☐ **Reference:**

ISO 27002 - 11.4.2 User Authentication for External Connections and 11.5.2 User identification and Authentication
NUIT ISSP/P - 3.2.3.3 NU Network Authentication, 3.2.2 Workforce Member Identification, 3.2.3 Workforce Member Authentication and 5.8 Remote Access

XVIII. Transmission Security 164.312(e)

XXXVIII. Integrity Controls

"Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of."

Addressable Actions:

Ensure that physical access to network equipment is restricted to only those that require access (e.g., network engineers, technical support personnel, etc.).
Establish local networks that permit adequate segregation and protection of ePHI data transmissions and traffic.
Use methods of data transmission and communication that help ensure adequate protection (e.g., virtual private network, secure file transfer protocol, data encryption, etc.).
Communicate securely the identities and passwords required for transmissions via encrypted communications (e.g., encrypted email) or using out-of-band methods (e.g., identity is emailed and the password is communicated via telephone).
Ensure the identity of the receiving party is known to you (e.g., use encryption keys that were previously and securely established).

☐ **Reference:**

ISO 27002 - 10.6.1 Network Controls and 10.9.2 On-Line
NUIT ISSP/P - 3.2.1 Access Authorization and 5.0 Network Security

XIX. Person or Entity Authentication 164.312(d)

XXXIX. Encryption

"Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate."

Addressable Actions:

Identify instances where the application of an encryption solution is appropriate
Implement a University-approved solution to help ensure data is protected.

☐ **Reference:**

ISO 27002 - 12.3.1 Policy on the Use of Cryptographic Controls
NUIT ISSP/P - 3.3.2 Data Encryption and 3.3.3 Securing Communications