# Introduction

This workbook contains all HIPAA Security Rule Standards and Implementation Specifications and when completed will provide procedure documentation for compliance. The UCCS Information Security Office is responsible for reviewing completed workbooks and identifying potential gaps. This document of compliance will be continually updated as we continue to improve our HIPAA compliance posture at UCCS.

# Instructions for Completing this Procedures Workbook

Each covered entity at UCCS shall complete the HIPAA entity information immediately below and all “Implemented Procedures:” boxes in this workbook. Each section labeled as “(Required)” corresponds to a section of the compliance standard that must be implemented as stated for compliance. For sections labeled “(Addressable)”, it must be determined whether each specification is reasonable and appropriate. If it is, it must be implemented as stated. If it is not, the entity must document the reasons for this determination and implement alternative compensating controls, or otherwise indicate how the intent of the standard can still be met. If a Standard or Implementation Specification does not apply, indicate “N/A” along with an explanation in that item’s “Implemented Procedures:” box.

While each entity is ultimately responsible for their compliance with the HIPAA Security Rule, in situations where UCCS OIT or another service provider is responsible for fulfilling one or more requirements. the HIPAA entity can request verification of implementation from the service provider where this documentation is not otherwise readily available. The HIPAA requirements for which a service provider is responsible must be clearly indicated in this workbook and in any attached documentation.

**HIPAA Entity Information**

|  |  |
| --- | --- |
| **HIPAA Entity Name:** |  |
| **Individual responsible for HIPAA Security Rule compliance:** | **Name & Title:**  |
| **Nature of electronic protected health information (ePHI) necessitating HIPAA Security Rule compliance:** |  |
| **List of systems, portable devices and electronic media that contain, access or transmit ePHI:**  |  |
| **Last update:**  | **Date:**   |
| **Reviewer Signatures:** |  |  |

**Table of Contents**

This document is arranged by HIPAA Security Rule requirements. Each implementation specification (or Standard in the absence of specific implementation specifications) is followed by practices for compliance, along with space to document implementation of the procedures and list other supporting documentation.

Introduction 1

HIPAA Security Rule: ADMINISTRATIVE STANDARDS 2

§164.308(a)(1)(i) - Security Management Process 2

§164.308(a)(2) - Assigned security responsibility 3

§164.308(a)(3)(i) - Workforce security 3

§164.308(a)(4)(i) - Information access management 4

§164.308(a)(5)(i) - Security awareness and training 5

§164.308(a)(6)(i) - Security incident procedures 7

§164.308(a)(7)(i) - Contingency plan 7

§164.308(a)(8) - Evaluation 9

§164.308(b)(1) - Business associate contracts and other arrangements 10

HIPAA Security Rule: PHYSICAL STANDARDS 10

§164.310(a)(1) - Facility access controls 10

§164.310(b) - Workstation use 12

§164.310(c) - Workstation security 12

§164.310(d)(1) - Device and media controls 13

HIPAA Security Rule: TECHNICAL STANDARDS 14

§164.312(a)(1) - Access Control 14

§164.312(b) - Audit controls 16

§164.312(c)(1) – Integrity 16

§164.312(d) - Person or entity authentication 17

§164.312(e)(1) - Transmission security 18

# HIPAA Security Rule: ADMINISTRATIVE STANDARDS

1. **STANDARD**

## §164.308(a)(1)(i) - Security Management Process

It is the responsibility of each UCCS Designated Health Care Component’s Leadership as well as the UCCS HIPAA Security Officer to implement policies and procedures to prevent, detect, contain, and correct security violations.

1. **§164.308(a)(1)(ii)(A) - Risk Analysis (Required)**

It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to 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 Designated Health Care Component.

**Practices for Compliance**

1. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to identify relevant information systems and electronic information resources that require protection.
2. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to conduct risk assessments to understand and document risks from security failures that may cause loss of confidentiality, integrity, or availability.  Risk assessments should take into account the potential adverse impact on the University’s reputation, operations, and assets. Risk assessments should include backups and non-original sources of ePHI.
3. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to review and update risk assessments every three years, or more frequently in response to significant legislative, environmental or operational changes.
4. It is the responsibility of each UCCS Designated Health Care Component’s Leadership to inform the UCCS HIPAA Privacy and Security Official(s) of the completion of all documented risk assessments within thirty (30) calendar days of their completion, and provide a copy upon request.

|  |
| --- |
| **Implemented Procedures:** |

1. **§164.308(a)(1)(ii)(B) - Risk Management (Required)**

It is the responsibility of each UCCS Designated Health Care Component’s Leadership, the UCCS Director of Campus Compliance / Privacy Officer, UCCS HIPAA Security Officer, and the Office of Information Technology to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.308(a).

**Practices for Compliance**

1. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to select appropriate controls, e.g. policies, procedures, technologies, to safeguard data relative to the sensitivity or criticality determined by the risk assessment, and document the party(ies) responsible for implementation of each recommended practice.
2. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to, where possible, incorporate these Standards and practices when evaluating and selecting new hardware and software.

|  |
| --- |
| **Implemented Procedures:** |

1. **§164.308(a)(1)(ii)(C) - Sanction Policy (Required)**

It is the responsibility of each UCCS Designated Health Care Component’s Leadership, the UCCS Director of Campus Compliance / Privacy Officer, UCCS HIPAA Security Officer, the Office of Information Technology, and the Human Resources Department to apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.

**Practices for Compliance**

1. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with Human Resources and College / Center Leadership to take disciplinary or other action in accordance with University personnel policies, bargaining agreements, and guidelines on workforce members who, during their employment, fail to comply with University policy and procedures, including information security policy and procedures.
2. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with Human Resources and College / Center Leadership to ensure that documentation of violations and application of HIPAA-related sanctions is maintained appropriately and retained for six years.
	* + - 1. HIPAA entities are responsible for informing Human Resources and/or Labor Relations when submitting documentation with this retention requirement.

|  |
| --- |
| **Implemented Procedures:** |

1. **§164.308(a)(1)(ii)(D) - Information system activity review (Required)**

It is the responsibility of each UCCS Designated Health Care Component’s Leadership as well as the UCCS HIPAA Security Officer to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

**Practices for Compliance**

1. It is the responsibility of each UCCS Designated Health Care Component’s Leadership or designee as well as the UCCS HIPAA Security Officer to regularly review information system activity and log-in attempts. The period for which activity logs are maintained and the extent, frequency, and nature of reviews are determined by the UCCS Designated Health Care Component’s security environment and overall security management process. The UCCS Security Officer will determine the period of review at least annually.
2. It is the responsibility of each UCCS Designated Health Care Component’s Leadership or designee as well as the UCCS HIPAA Security Officer to maintain documentation of periodic log reviews.
3. Logs relevant to security incidents should be retained for six years and the remainder of the data should only be retained for up to 90 days in accordance with usual and customary practice.
4. It is the responsibility of each UCCS Designated Health Care Component’s Leadership as well as the UCCS HIPAA Security Officer to define responsibility for information system activity review, including log-in monitoring and access reports.

|  |
| --- |
| **Implemented Procedures:** |

* + 1. **STANDARD**

## §164.308(a)(2) - Assigned security responsibility

It is the responsibility of each UCCS Designated Health Care Component’s Leadership to identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.

|  |
| --- |
| **Implemented Procedures:** |

* + 1. **STANDARD**

## §164.308(a)(3)(i) - Workforce security

It is the responsibility of each UCCS Designated Health Care Component’s Leadership as well as the UCCS HIPAA Security Officer, and the Office of Information Technology to implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a) (4) of this section, and to prevent those workforce members who do not have access under paragraph (a) (4) of this section from obtaining access to electronic protected health information.

1. **§164.308(a)(3)(ii)(A) - Authorization and/or supervision (Addressable)**

It is the responsibility of each UCCS Designated Health Care Component’s Leadership as well as the UCCS HIPAA Security Officer to 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.

**Practices for Compliance**

1. It is the responsibility of each UCCS Designated Health Care Component’s Leadership to determine which individuals are authorized to work with ePHI in accordance with a role-based approach.

|  |
| --- |
| **Implemented Procedures:** |

1. **§164.308(a)(3)(ii)(B) - Workforce clearance procedure (Addressable)**

It is the responsibility of each UCCS Designated Health Care Component’s Leadership as well as the UCCS HIPAA Security Officer to implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

**Practices for Compliance**

1. It is the responsibility of each UCCS Designated Health Care Component’s Leadership, or designee, to review role definitions and assignments for appropriateness at least annually.
2. It is the responsibility of each UCCS Designated Health Care Components Leadership, or designee, to review access management procedures for appropriateness at least annually.

|  |
| --- |
| **Implemented Procedures:** |

1. **§164.308(a)(3)(ii)(C) - Termination procedures (Addressable)**

It is the responsibility of each UCCS Designated Health Care Component’s Leadership as well as the UCCS Office of Information Technology in conjunction with the Human Resources Department to implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a) (3) (ii) (B) of this section.

**Practices for Compliance**

1. It is the responsibility of each UCCS Designated Health Care Component’s Leadership as well as the UCCS HIPAA Security Officer to establish account maintenance procedures that ensure termination of accounts or change in access privileges for individuals who have been terminated or are no longer authorized to access ePHI.

|  |
| --- |
| **Implemented Procedures:** |

* + 1. **STANDARD**

## §164.308(a)(4)(i) - Information access management

It is the responsibility of each UCCS Designated Health Care Component’s Leadership as well as the UCCS HIPAA Security Officer to implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

1. **§164.308(a)(4)(ii)(A) - Isolating health care clearinghouse functions (Required)**

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.

|  |
| --- |
| **Implemented Procedures:** |

1. **§164.308(a)(4)(ii)(B) - Access authorization (Addressable)**

It is the responsibility of each UCCS Designated Health Care Component’s Leadership to 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.

**Practices for Compliance**

1. It is the responsibility of each UCCS Designated Health Care Component’s Leadership as well as the UCCS HIPAA Security Officer to ensure there is a formal system for authorizing user access to ePHI, such as an account request form requiring management approval.
2. It is the responsibility of each UCCS Designated Health Care Component’s Leadership to ensure access is to be granted in accordance with a role-based approach.
3. It is the responsibility of each UCCS Designated Health Care Component’s Leadership to maintain documentation of all authorized users of ePHI and their access levels.
4. It is the responsibility of each UCCS Designated Health Care Component’s Leadership to ensure workforce members must receive security awareness and HIPAA training prior to obtaining access to ePHI.
5. It is the responsibility of each UCCS Designated Health Care Component’s Leadership as well as the UCCS HIPAA Security Officer to ensure HIPAA systems must have the capacity to set access controls.

|  |
| --- |
| **Implemented Procedures:** |

1. **§164.308(a)(4)(ii)(C) - Access establishment and modification (Addressable)**

It is the responsibility of each UCCS Designated Health Care Component’s Leadership as well as the UCCS HIPAA Security Officer to 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.

**Practices for Compliance**

1. It is the responsibility of each UCCS Designated Health Care Component’s Leadership as well as the UCCS HIPAA Security Officer and the UCCS Office of Information technology to develop and implement procedures to establish, document, review and modify a user’s access to ePHI. Access shall use the principle of “least privileges.”
2. It is the responsibility of each UCCS Designated Health Care Component’s Leadership as well as the UCCS HIPAA Security Officer to ensure procedures include a regular review of those with access to ePHI, including the appropriateness of access levels. The period for which and the extent, frequency, and nature of reviews are determined by the UCCS Designated Health Care Component’s security environment and overall security management process. The UCCS Security Officer will determine the period of review at least annually.
3. It is the responsibility of each UCCS Designated Health Care Component’s Leadership as well as the UCCS HIPAA Security Officer and the UCCS Office of Information Technology to ensure procedures must require prompt initiation of account modifications/termination.

|  |
| --- |
| **Implemented Procedures:** |

* + 1. **STANDARD**

## §164.308(a)(5)(i) - Security awareness and training

It is the responsibility of each UCCS Designated Health Care Component’s Leadership as well as the UCCS Director of Campus Compliance / HIPAA Privacy Office and the HIPAA Security Officer to implement a security awareness and training program for all members of its workforce (including management).

1. **§164.308(a)(5)(ii)(A) - Security reminders (Addressable)**

It is the responsibility of each UCCS Designated Health Care Component’s Leadership as well as the UCCS HIPAA Security Officer to ensure periodic security updates.

**Practices for Compliance**

1. It is the responsibility of each UCCS Designated Health Care Component’s Leadership as well as the UCCS HIPAA Security Officer to establish security awareness and HIPAA training for all members of the UCCS workforce who are involved in the creation, transmission, and storage of ePHI. Training activities include:
2. Initial security awareness and HIPAA training for individuals with ePHI-related job duties. Training will include UCCS Password Standards and the importance of protecting against malicious software and exploitation of vulnerabilities.
3. Review of changes to internal policies, procedures, and technologies
4. Periodic reminders about security awareness and HIPAA
5. Security notices or updates regarding current threats
6. It is the responsibility of each UCCS Designated Health Care Component’s Leadership as well as the UCCS HIPAA Security Officer to ensure HIPAA entities must maintain records of training materials and completion of training for six years.

|  |
| --- |
| **Implemented Procedures:** |

1. **§164.308(a)(5)(ii)(B) - Protection from malicious software (Addressable)**

It is the responsibility of the UCCS HIPPA Security Officer in conjunction with the UCCS Information Technology Department to develop procedures for guarding against, detecting, and reporting malicious software.

**Practices for Compliance**

1. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the UCCS Information Technology Department to protect all devices against malicious software, such as computer viruses, Trojan horses, spyware, etc.,. Also ensure the safeguards and appropriate configurations are included in the standard set-up procedures for new systems and workstations that contain or access ePHI.
2. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the UCCS Information Technology Department to run versions of operating system and application software for which security patches are made available and installed in a timely manner in accordance with [UCCS Security Standards for Information Systems](https://www.uccs.edu/oit/security/security-program/security-standards). The UCCS Security Officer will determine the period of review at least annually.
3. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the UCCS Information Technology Department to harden systems. “Hardening” includes:
	1. Install OS and third-party application updates (patches) and keep them current
	2. Change or remove default logins/passwords
	3. Disable unnecessary services
	4. Install virus and malware protection software and update them at least weekly
	5. Set proper file/directory ownership/permissions;
4. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the UCCS Information Technology Department to periodically, and at least annually, review HIPAA workstation browser settings to ensure that they comply with [UCCS Security Standards for Information Systems](https://www.uccs.edu/oit/security/security-program/security-standards) and [UCCS Policy 700-002 Responsible Computing Section II.B.1.a.](https://www.uccs.edu/vcaf/sites/vcaf/files/inline-files/700-002.pdf)
5. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the UCCS Information Technology Department to periodically, and at least annually, review email client settings to ensure they comply with current UCCS Office of Information Technology recommendations.
6. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the UCCS Information Technology Department to perform periodic network vulnerability scans of systems containing known ePHI, and workstations that access ePHI, and take adequate steps to correct discovered vulnerabilities.
7. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the UCCS Information Technology Department to implement e-mail malicious code filtering.
8. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the UCCS Information Technology Department to install/enable firewalls (hardware and/or software) to reduce threat of unauthorized remote access.
9. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the UCCS Information Technology Department to ensure intrusion detection software and/or systems may also be installed to detect threat of unauthorized remote access.

|  |
| --- |
| **Implemented Procedures:** |

1. **§164.308(a)(5)(ii)(C) - Log-in monitoring (Addressable)**

It is the responsibility of each UCCS Designated Health Care Component’s Leadership as well as the UCCS HIPAA Security Officer to ensure procedures for monitoring log-in attempts and reporting discrepancies.

**Practices for Compliance**

See §164.308(a)(1)(ii)(D) - Information system activity review, above.

|  |
| --- |
| **Implemented Procedures:** |

1. **§164.308(a)(5)(ii)(D) - Password management (Addressable)**

It is the responsibility of each UCCS Designated Health Care Component’s Leadership as well as the UCCS HIPAA Security Officer in conjunction with the UCCS Office of Information Technology to develop procedures for creating, changing, and safeguarding passwords.

**Practices for Compliance**

1. Passwords for systems containing or accessing ePHI will comply with the UCCS Password Strength and Security Standards.
2. It is the responsibility of each UCCS Designated Health Care Component’s Leadership to enforce UCCS password complexity requirements for third-party access as possible.

|  |
| --- |
| **Implemented Procedures:** |

* + 1. **STANDARD**

## §164.308(a)(6)(i) - Security incident procedures

It is the responsibility of each UCCS Designated Health Care Component’s Leadership as well as the UCCS HIPAA Security Officer in conjunction with UCCS Office of Information Technology Department to implement policies and procedures to address security incidents.

1. **§164.308(a)(6)(ii) - Response and Reporting (Required)**

It is the responsibility of each UCCS Designated Health Care Component’s Leadership as well as the UCCS HIPAA Security Officer in conjunction with UCCS Office of Information Technology Department to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the UCCS Designated Health Care Component; and document security incidents and their outcomes.

**Practices for Compliance**

1. Suspected or known security incidents involving ePHI must be reported to the campus HIPAA Security Officer. (Note: Privacy incidents involving ePHI must be reported to the UCCS Director of Campus Compliance / HIPAA Privacy Officer.) See *§164.308(a)(2) - Assigned security responsibility*, above.
2. It is the responsibility of each UCCS Designated Health Care Component’s Leadership to have procedures and training in place to ensure that suspected or known security incidents involving ePHI are reported and documented appropriately as per Attachment 2 Documentation Policy (Retention).
3. Security incidents determined to involve ePHI must be documented, tracked and reported as defined in HIPAA entity documentation and UCCS [Guidelines for Reporting Information Security Incidents](https://www.uccs.edu/oit/security/incident-response).

|  |
| --- |
| **Implemented Procedures:**Follow the incident response and reporting as described in the IT Security Website. Report immediately to HIPAA Office and HIPAA Security Officer. |

* + 1. **STANDARD**

## §164.308(a)(7)(i) - Contingency plan

It is the responsibility of each UCCS Designated Health Care Component’s Leadership as well as the UCCS HIPAA Security Officer in conjunction with UCCS Office of Information Technology Department to establish (and implement as needed) policies and procedures for responding an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

1. **§164.308(a)(7)(ii)(A) - Data backup plan (Required)**

It is the responsibility of each UCCS Designated Health Care Component’s Leadership as well as the UCCS HIPAA Security Officer in conjunction with UCCS Office of Information Technology Department to establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

**Practices for Compliance**

1. It is the responsibility of each UCCS Designated Health Care Component’s Leadership to ensure back up original sources of essential ePHI on an established schedule.
2. It is the responsibility of each UCCS Designated Health Care Component’s Leadership to ensure backup copies are securely stored in a physically separate location from the data source.
3. It is the responsibility of each UCCS Designated Health Care Component’s Leadership to ensure backups containing ePHI will be transported via secure methods.
4. It is the responsibility of each UCCS Designated Health Care Component’s Leadership to ensure documentation exists to verify the creation of backups and their secure storage.

|  |
| --- |
| **Implemented Procedures:** |

1. **§164.308(a)(7)(ii)(B) - Disaster recovery plan (Required)**

It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to establish (and implement as needed) procedures to restore any loss of data.

**Practices for Compliance**

1. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to establish procedures to restore loss of essential ePHI as a result of a disaster or emergency.
2. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to maintain copies of the data restoration procedures that are readily accessible at more than one location and should not rely on the availability of local power or network.
3. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to develop backup procedures that must include steps to ensure that all protections (patches, configurations, permissions, firewalls, etc.) are re-applied and restored before ePHI is restored to a system.

|  |
| --- |
| **Implemented Procedures:** |

1. **§164.308(a)(7)(ii)(C) - Emergency mode operation plan (Required)**

It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to 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.

**Practices for Compliance**

1. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to ensure that HIPAA entity emergency operations procedures maintain security protections for ePHI.
2. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to evaluate operations in emergency mode, e.g. a technical failure or power outage, to determine whether security processes to protect ePHI are maintained.
3. It is the responsibility of each UCCS Designated Health Care Component’s Leadership to document assessment and conclusions.
4. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to document and implement additional authorities and procedures necessary to ensure the continuation of security protections for ePHI during emergency operations mode.
5. It is the responsibility of each UCCS Designated Health Care Component’s Leadership to develop plans for evacuations:
	1. UCCS Designated Health Care Component’s entities’ emergency response plans shall include logging out of systems that contain ePHI, securing files, and locking up before evacuating a building, if safe to do so.
	2. UCCS Designated Health Care Components should have processes to ensure there was no breach when the area is re-occupied.

|  |
| --- |
| **Implemented Procedures:** |

1. **§164.308(a)(7)(ii)(D) - Testing and revision procedures (Addressable)**

It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to implement procedures for periodic testing and revision of contingency plans.

**Practices for Compliance**

* 1. It is the responsibility of each UCCS Designated Health Care Component’s Leadership to document the contingency plan procedures.
	2. It is the responsibility of each UCCS Designated Health Care Component’s Leadership to ensure that those responsible for executing contingency plan procedures understand their responsibilities.

3. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to periodically, and at least annually, perform a test of the contingency plan procedures.

4. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to document test results, review and correct any problems with the test, and update procedures accordingly.

|  |
| --- |
| **Implemented Procedures:** |

1. **§164.308(a)(7)(ii)(E) - Applications and data criticality analysis (Addressable)**

It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to assess the relative criticality of specific applications and data in support of other contingency plan components.

**Practices for Compliance**

1. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to prioritize criticality of applications and data sets for data back-up, restoration, and application of emergency mode operation plan.
2. Priorities can be included in data restoration procedures (*§164.308(a)(7)(ii)(B) - Disaster recovery plan*)

|  |
| --- |
| **Implemented Procedures:** |

* + 1. **STANDARD**

## §164.308(a)(8) - Evaluation

It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational 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.

**Practices for Compliance**

 1. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer and the UCCS Director of Campus Compliance / HIPAA Privacy Officer to review and update campus HIPAA Policy and Practices for Compliance every five (5) years, or more frequently in response to environmental or operational changes that affect the security of ePHI.

* 1. Submit to the UCCS HIPAA Security Officer and the UCCS Director of Campus Compliance / HIPAA Privacy Officer once annually by calendar year-end a list of titles and last revision dates of the policies designed to meet HIPAA Security Rule requirements, and provide copies upon request.

 2. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer and the UCCS Director of Campus Compliance / HIPAA Privacy Officer to review and update Unit policies and procedures annually if there is no trigger for more frequent review.

1. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer and the UCCS Director of Campus Compliance / HIPAA Privacy Officer to identify the individual(s) responsible for determining when evaluation is necessary due to environmental or operational changes.
2. Document periodic reviews the updates and archive previous versions. Retain for six years as per Attachment 2 Documentation Policy (Retention).

|  |
| --- |
| **Implemented Procedures:** |

**IX. STANDARD**

## §164.308(b)(1) - Business associate contracts and other arrangements

A covered entity, in accordance with §164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity’s behalf only if the covered entity obtains satisfactory assurances, in accordance with §164.314(a) that the business associate will appropriately safeguard the information.

1. **§164.308(b)(4) - Written contract or other arrangement (Required)**

It is the responsibility of each UCCS Designated Health Care Component’s Leadership to document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a).

**Practices for Compliance**

1. It is the responsibility of each UCCS Designated Health Care Component’s Leadership to ensure that agreements with business associates [[1]](#footnote-1) contain language stating that University ePHI receives appropriate safeguards in accordance with Federal HIPAA Security Regulations.
2. It is the responsibility of each UCCS Designated Health Care Component’s Leadership to use the UCCS Business Associate Agreements (BAA) template or send the third parties BAA to both UCCS Legal Counsel and Director of Campus Compliance / HIPAA Privacy Officer for review prior to signing.
3. It is the responsibility of each UCCS Designated Health Care Component’s Leadership to ensure that UCCS-approved BAAs are in place at either a System-wide or local level for vendors and third-party service providers with access to UCCS ePHI or to systems that contain or access ePHI.
4. HIPAA entity procedures must include notifying Procurement Services when a HIPAA BAA is needed and when renewing an agreement with an existing HIPAA BAA.

|  |
| --- |
| **Implemented Procedures:** |

# HIPAA Security Rule: PHYSICAL STANDARDS

**X. STANDARD**

## §164.310(a)(1) - Facility access controls

It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

1. **§164.310(a)(2)(i) - Contingency Operations (Addressable)**

It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to 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.

**Practices for Compliance**

* 1. It is the responsibility of each UCCS Designated Health Care Component’s Leadership to ensure that contingency procedures and authorization (See *§164.308(a)(7)(i): Administrative Standards – Contingency Plan*) include facility access.

|  |
| --- |
| **Implemented Procedures:** |

1. **§164.310(a)(2)(ii) - Facility security plan (Addressable)**

It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer, UCCS Director of Campus Compliance / HIPAA Privacy Officer, and UCCS Facilities Services to implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

**Practices for Compliance**

* 1. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to ensure systems and electronic media containing ePHI are to be located in physically secure locations. A secure location would minimally be defined as one that is not routinely accessible to the public, particularly if authorized personnel are not always available to monitor security.

2. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS Facilities Services to ensure that secure locations have physical access controls (card key, door locks, alarms, etc.) that prevent unauthorized entry, particularly during periods outside of normal work hours, or when authorized personnel are not present to monitor security. If logging is available, it should be enabled.

1. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to ensure access control systems are maintained in good working order.
2. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with Facilities Services to ensure the facility security plans document use of physical access controls.

|  |
| --- |
| **Implemented Procedures:** |

1. **§164.310(a)(2)(iii) - Access control and validation procedures (Addressable)**

It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer and the UCCS Director of Campus Compliance / HIPAA Privacy Officer to 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.

**Practices for Compliance**

* 1. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to develop an access plan for facilities containing ePHI that utilizes role- or function-based access control, including for visitors, service providers, and contractors.
	2. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to ensure the role- or function-based access control and validation procedures are closely aligned with the facility security plan.
	3. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to ensure the security plan for facilities containing ePHI includes key systems or electronic door access.
1. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer, the UCCS Director of Campus Compliance / HIPAA Privacy Officer, UCCS Facility Services, and Human Resources to conduct a periodic (at least annual) review and implementation of termination procedures, which may include a review of key inventory or electronic door access, to ensure currency of access authorization.

|  |
| --- |
| **Implemented Procedures:** |

**§164.310(a)(2)(iv) - Maintenance records (Addressable)**

It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS Facility Services Department to 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).

**Practices for Compliance**

* 1. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS Facility Services Department to develop policy and procedure for maintaining a record of any maintenance repairs and modifications to physical components of a facility containing ePHI related to security, such as hardware, walls, doors, and locks.
	2. Documentation should contain appropriate detail for review, including date, repair, and/or modification(s) made, and the contractor.
	3. Documentation should be stored securely.
	4. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS Facility Services Department to identify party(ies) responsible for recording and maintaining these records.

|  |
| --- |
| **Implemented Procedures:** |

**XI. STANDARD**

## §164.310(b) - Workstation use

It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to 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 that can access ePHI.

**Practices for Compliance**

* 1. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to ensure functions to be performed on workstations containing or accessing ePHI are aligned with roles.
	2. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to develop policies and procedures that specify where to place and position workstations to only allow viewing by authorized individuals, as well as additional privacy measures, commensurate with the risk of exposure.
	3. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to ensure unencrypted ePHI will not be stored on portable electronic devices, including laptops.
	4. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to ensure storage of ePHI on non-university equipment is forbidden, except in the case of storage by a third party with a HIPAA BAA.
1. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer and the UCCS Office of Information Technology to ensure remote access of ePHI will utilize secure channels.

|  |
| --- |
| **Implemented Procedures:** |

**XII. STANDARD**

## §164.310(c) - Workstation security

It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

**Practices for Compliance**

1. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to ensure all workstations, including laptops, containing ePHI are to be physically secured (locked down).
2. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to ensure all workstations and electronic devices that contain or access ePHI will be identified, such as laptops, desktop computers, and personal digital assistants (PDAs).
3. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to ensure unencrypted ePHI will not be stored on portable electronic devices, including laptops.
4. If ePHI is stored on removable media, additional physical controls must be implemented, such as ensuring that the device is physically secured or in the physical possession of the responsible party. Encryption is a compensating control for these additional measures.

|  |
| --- |
| **Implemented Procedures:** |

**XIII. STANDARD**

## §164.310(d)(1) - Device and media controls

It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility.

1. **§164.310(d)(2)(i) - Disposal (Required)**

It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to implement policies and procedures to address the final disposition of ePHI, and/or the [hardware or electronic media](https://www.uccs.edu/vcaf/sites/vcaf/files/inline-files/700-006.pdf) on which it is stored.

**Practices for Compliance**

* 1. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to ensure that ePHI on hardware and electronic media, including copiers, faxes, printers, etc., is unusable and/or inaccessible prior to disposal, including disposal by a Business Associate[[2]](#footnote-2).
	2. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to follow [UCCS Policy 700-006 Computer and Electronics Disposal](https://www.uccs.edu/vcaf/sites/vcaf/files/inline-files/700-006.pdf).
	3. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to ensure when portable media is discarded, it must either be overwritten in accordance with National Institute of Standards and Technology (NIST) guidelines, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>, or physically destroyed, eliminating all possibility that any ePHI contents could be read.

4. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to ensure when a system is recycled, transferred to another user not authorized for the data, or discarded, all storage devices or all ePHI records must be overwritten in accordance with NIST guidelines (link above), or physically destroyed, rendering all ePHI records unreadable.

|  |
| --- |
| **Implemented Procedures:** |

1. **§164.310(d)(2)(ii) - Media re-use (Required)**

It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to implement procedures for removal of ePHI from electronic media before the media are made available for re-use.

**Practices for Compliance**

* 1. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to ensure that ePHI on hardware and electronic media is unusable and/or inaccessible prior to re-use.
1. When a system is recycled or transferred to another user not authorized for the data, or otherwise re-used outside of a HIPAA-compliant environment, all storage devices or all ePHI records must be overwritten in accordance with National Institute of Standards and Technology (NIST) guidelines, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>, rendering all ePHI records unreadable.

|  |
| --- |
| **Implemented Procedures:** |

1. **§164.310(d)(2)(iii) - Accountability (Addressable)**

It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to maintain a record of the movements of hardware and electronic media and any person responsible therefore.

**Practices for Compliance**

* 1. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to maintain a record of the movements of, and person(s) responsible for, hardware and electronic media containing ePHI.
		+ - 1. Identify all types of hardware and electronic media that must be tracked.
		1. Special attention must be paid to portable devices and removable media. These devices should not ordinarily contain ePHI and must be individually identified in the tracking system in order to contain ePHI. Their use must be consistent with the individual’s identified role, such as according to a role-based matrix.
		2. This inventory should be physically confirmed at least annually.
			+ 1. Tracking system must include a mechanism for documenting the initial assignment of responsibility for devices that contain ePHI, as well as the transfer of authority for these devices.

2. Transport of archival media between the origination point and remote storage location must use a secure method to avoid unauthorized access to the archival media.

1. Loss or theft of electronic equipment or media containing ePHI must immediately be reported according to campus incident response procedures. <https://www.uccs.edu/oit/security/incident-response>. Also see §164.308(a)(6)(i) - Security incident procedures.

|  |
| --- |
| **Implemented Procedures:** |

1. **§164.310(d)(2)(iv) - Data backup and storage (Addressable)**

It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to create a retrievable, exact copy of ePHI, when needed, before movement of equipment.

**Practices for Compliance**

* + 1. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to create a retrievable, exact copy of original sources of essential ePHI before moving equipment containing them.

2. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to establish a process for documenting or verifying creation of retrievable, exact copy of original sources of essential ePHI.

1. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to develop retrievable, exact copies of ePHI that must be protected in accordance with these Standards.

|  |
| --- |
| **Implemented Procedures:** |

# HIPAA Security Rule: TECHNICAL STANDARDS

**XIV. STANDARD**

## §164.312(a)(1) - Access Control

It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)

**§164.312(a)(2)(i) - Unique user identification (Required)**

It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to assign a unique name and/or number for identifying and tracking user identity.

**Practices for Compliance**

* 1. Each User must be provided a unique account, with a unique username/user ID and password, for access to ePHI.
	2. Generic or shared accounts are not permitted for access to ePHI.

|  |
| --- |
| **Implemented Procedures:** |

**§164.312(a)(2)(ii) - Emergency access procedure (Required)**

It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.

**Practices for Compliance**

* 1. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to establish procedures to ensure that necessary ePHI can be accessed during an emergency.
	2. Emergency access procedures may be included in Contingency Plan procedures (see §164.308(a)(7)(i) - Contingency plan).
	3. It is the responsibility of each UCCS Designated Health Care Component’s Leadership in conjunction with the UCCS HIPAA Security Officer to develop emergency access procedures that shall be written and communicated in advance to multiple individuals within the organization.
	4. It is the responsibility of each UCCS Designated Health Care Component’s Leadership to ensure emergency access procedures should not rely on the availability of a single individual.
	5. It is the responsibility of each UCCS Designated Health Care Component’s Leadership to ensure access to emergency procedures should not rely on the availability of local power or network.
	6. It is the responsibility of each UCCS Designated Health Care Component’s Leadership to identify roles that may require special access during an emergency.
		1. Individuals are to require proper ID or other official verification before granting access to unknown or not-normally-authorized individuals in emergency circumstances.

|  |
| --- |
| **Implemented Procedures:** |

**§164.312(a)(2)(iii) - Automatic logoff (Addressable)**

It is the responsibility of the UCCS HIPAA Security Officer in conjunction with each UCCS Designated Health Care Component’s Leadership to implement electronic procedures that terminate an electronic session after a predetermined time of inactivity as per section XIV.D.3 below.

**Practices for Compliance**

* 1. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with each UCCS Designated Health Care Component’s Leadership to ensure where possible, that electronic sessions terminate after a period of inactivity.
	2. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with each UCCS Designated Health Care Component’s Leadership to ensure, where session termination is not possible, either technically or from a business process perspective, automatic workstation lockout is implemented as a compensating control.
	3. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with each UCCS Designated Health Care Component’s Leadership to ensure a maximum duration of inactivity prior to session termination or automatic workstation lockout is 10 minutes. *Note: The UCCS Information Security Office may consider written requests for exceptions to the 10-minute requirement. These requests will be kept on file for 6 years.*

|  |
| --- |
| **Implemented Procedures:** |

**§164.312(a)(2)(iv) - Encryption and decryption (Addressable)**

It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology to implement a mechanism to encrypt and decrypt ePHI.

**Practices for Compliance**

* + 1. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology to implement appropriate security measures, such as encryption, to protect ePHI from unauthorized access.
			1. Unencrypted ePHI will not be stored on portable electronic devices, including laptops (see §164.310(b) - Workstation use and §164.310(c) - Workstation security).
		2. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology to, in situations where encryption is problematic, implement the alternative compensating controls below as appropriate.
			1. It is the responsibility of the UCCS HIPAA Security Officer to keep an explanation for why encryption is not being implemented.
			2. **Alternative, reasonable and appropriate compensating controls if encryption is not in place for stored ePHI:**
		3. Access controls, including unique user ID & password authentication, and user profiles
		4. Hardening of systems (see §164.308(a)(5)(ii)(B) - for details)
		5. Physical security for access to facilities and workstations that contain or access ePHI, including appropriate device and media controls
		6. Technically enforce complex passwords where possible
		7. Enable system security auditing/logging, including monitoring of audit reports/logs
		8. Correct configuration of applications to use secure protocols
		9. Implement automatic logoff and/or screen lock (see §164.312(a)(2)(iii) - for details)
		10. Ensure secure remote access
		11. Implement correctly configured firewalls (hardware and/or software)

|  |
| --- |
| **Implemented Procedures:** |

**XV. STANDARD**

## §164.312(b) - Audit controls

It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component’s Leadership, to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

**Practices for Compliance**

* 1. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component’s Leadership, to establish criteria for log creation, retention, and examination of activity.
	2. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component’s Leadership, to review that new systems should be selected with the ability to support audit requirements.
	3. See §164.308(a)(1)(ii)(D) - Information system activity review for additional administrative practices.

|  |
| --- |
| **Implemented Procedures:** |

**XVI. STANDARD**

## §164.312(c)(1) – Integrity

It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component’s Leadership, to implement policies and procedures to protect ePHI from improper alteration or destruction.

1. **§164.312(c)(2) - Mechanism to authenticate electronic protected health information (Addressable)**

It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component’s Leadership, to implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.

**Practices for Compliance**

1. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component’s Leadership, to leverage application-specific mechanisms or functionality when available to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.
2. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component’s Leadership, to regularly review access logs for unauthorized direct access or administrator/root access to table data containing ePHI. The frequency at which activity logs are reviewed and the extent, frequency, and nature of reviews are determined by the UCCS Designated Health Care Component’s security environment and overall security management process.
3. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component’s Leadership, to implement the following practices as a means of protecting ePHI from being altered or destroyed in an unauthorized manner:
	1. Ensure appropriate physical security is in place for devices that contain or access ePHI (see *Physical Security Standards*).
	2. Protect all devices against malicious software (see *§164.308(a)(5)(ii)(B) - Protection from malicious software* for details).
	3. Protect sensitive data with appropriate strategies, such as secure file transfer *(§164.312(e)(1) - Transmission security*) and use of web browser security standards *(§164.308(a)(5)(ii)(B)) - Protection from malicious software*).
	4. Implement processes to notify users and take other appropriate remedial action in the event of propagation of malicious software (see *§164.308(a)(5)(ii)(A) - Security reminders*).

|  |
| --- |
| **Implemented Procedures:** |

**XVII. STANDARD**

## §164.312(d) - Person or entity authentication

It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component’s Leadership, to implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

**Practices for Compliance**

1. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component’s Leadership, to ensure each User must be provided a unique account, with a unique User Name/ID and Password, for access to ePHI.
	1. Generic or shared accounts are not permitted for access to ePHI.
	2. Passwords for access to ePHI will not be shared by UCCS Employees or Workforce Members.
	3. All passwords providing access to ePHI, including local administrator/root passwords, must comply with the UCCS [Policy on Responsible Computing 700-002](https://www.uccs.edu/vcaf/sites/vcaf/files/inline-files/700-002.pdf)
	4. Physically protect passwords
2. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component’s Leadership, to review, as appropriate, workstation, OS and application access logs, as well as failed or successful changes to account permissions (*also see §164.308(a)(1)(ii)(D) - Information system activity review*).
3. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component’s Leadership, to ensure systems and applications will not be configured to save passwords.
4. All of the above practices apply to vendors and third parties.

|  |
| --- |
| **Implemented Procedures:** |

**XVIII. STANDARD**

## 164.312(e)(1) - Transmission security

It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component’s Leadership, to implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.

1. **§164.312(e)(2)(i) - Integrity controls (Addressable)**

It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component’s Leadership, to implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.

**Practices for Compliance**

* + 1. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component’s Leadership, to ensure wired and wireless transmission of ePHI will use secure protocols (encryption).
		2. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component’s Leadership, to ensure all remote access of ePHI must be by secure methods only.

3. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component’s Leadership, to ensure unprotected ePHI shall not be sent via unencrypted email.

* 1. Note: It is acceptable to send ePHI via email in encrypted, password-protected attachments to known business partners, and in response to legitimate requests if no secure channel exists.

4. It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component’s Leadership, to ensure received email containing ePHI is adequately deleted when there is no longer a business need to retain it. Procedures are available in individual HIPAA entity training or as requested of the OIT helpdesk.

1. UCCS Workforce Members must delete or redact ePHI from the body of received email before replying to it.

|  |
| --- |
| **Implemented Procedures:** |

1. **§164.312(e)(2)(ii) – Encryption (Addressable)**

It is the responsibility of the UCCS HIPAA Security Officer in conjunction with the Office of Information Technology, and if necessary each UCCS Designated Health Care Component’s Leadership, to implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

See *§164.312(e)(2)(i) - Integrity controls (Addressable)*, above, for recommended practices.

**Note:** Also see *§164.312(a)(2)(iv) – Encryption and decryption (Addressable)*, above, for storage of ePHI.

|  |
| --- |
| **Implemented Procedures:** |

1. A “business associate” is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or as a service to, a covered entity. This includes services where disclosure of ePHI is not limited in nature, such as destruction services or a software vendor that needs access to ePHI in order to provide its service. Common exclusions include health care providers that must comply with HIPAA requirements, conduits (physical or electronic) that transport but do not access protected health information, custodial services, destruction services when the work is performed under the direct control of the covered entity (in which case the service may be treated as part of the workforce). For additional clarification, inclusions and exclusions, see <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html> and <http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf>, page 8378, column 1, (b)(1). [↑](#footnote-ref-1)
2. Also see §164.308(b)(1), Business associate contracts and other arrangements [↑](#footnote-ref-2)