ITS HIPAA Security Compliance Recommendations

October 24, 2005
Updated May 31, 2010

http://its.uncc.edu/HIPAA/Security/
# Table of Contents

**Introduction** .................................................................................................................. 1  
  Purpose of this Document ................................................................................................. 1  
  Important Terms ................................................................................................................. 1  
  Organization of this Document ........................................................................................ 1  
  Standards and Implementation Specifications ................................................................. 2  
  Covered Entities and Business Associates .................................................................... 2  
  **§164.308 Administrative Safeguards** ........................................................................... 3  
  §164.308 (a)(1)(i) Security Management Process .......................................................... 3  
  §164.308 (a)(1)(ii)(A) Risk Analysis ................................................................................ 4  
  §164.308 (a)(1)(ii)(B) Risk Management ........................................................................ 4  
  §164.308 (a)(1)(ii)(C) Sanction Policy .............................................................................. 5  
  §164.308 (a)(1)(ii)(D) Information System Activity Review ........................................... 5  
  §164.308 (a)(2) Assigned Security Responsibility .......................................................... 6  
  §164.308 (a)(3)(i) Workforce Security ............................................................................ 7  
  §164.308 (a)(3)(ii)(A) Authorization and/or Supervision .............................................. 7  
  §164.308 (a)(3)(ii)(B) Workforce Clearance Procedures .............................................. 8  
  §164.308 (a)(3)(ii)(C) Termination Procedures ............................................................... 9  
  §164.308 (a)(4)(i) Information Access Management ...................................................... 10  
  §164.308 (a)(4)(ii)(A) Isolating Healthcare Clearinghouse functions .......................... 10  
  §164.308 (a)(4)(ii)(B) Access Authorization ................................................................. 11  
  §164.308 (a)(4)(ii)(C) Access Establishment and Modification ...................................... 11  
  §164.308 (a)(5)(i) Security Awareness and Training .................................................... 12  
  §164.308 (a)(5)(ii)(A) Security Reminders ................................................................. 12  
  §164.308 (a)(5)(ii)(B) Protection from Malicious Software .......................................... 13  
  §164.308 (a)(5)(ii)(C) Log-in Monitoring .................................................................... 13  
  §164.308 (a)(5)(ii)(D) Password Management ............................................................. 14  
  §164.308 (a)(6)(i) Security Incident Procedures and §164.308 (a)(6)(ii) Response and  
  Reporting ......................................................................................................................... 14  
  §164.308 (a)(7)(i) Contingency (Business Continuity) Plan .......................................... 15  
  §164.308 (a)(7)(ii)(A) Data Backup Plan ...................................................................... 16  
  §164.308 (a)(7)(ii)(B) Disaster Recovery Plan ............................................................. 16  
  §164.308 (a)(7)(ii)(C) Emergency Mode Operations Plan .......................................... 17  
  §164.308 (a)(7)(ii)(D) Testing and Revision Procedures ............................................. 17  
  §164.308 (a)(7)(ii)(E) Application and Data Criticality Analysis .................................. 18  
  §164.308 (a)(8) Evaluation ......................................................................................... 18  
  §164.308 (b)(1) Business Associate Contracts and Other Arrangements .................. 19  
  §164.308 (b)(4) Written Contract or Other Arrangement ............................................. 19  
  **§164.310 Physical Safeguards** .................................................................................... 19  
  §164.310 (a)(1) Facility Access Controls ....................................................................... 19  
  §164.310 (a)(2)(i) Contingency Operations ................................................................... 20  
  §164.310 (a)(2)(ii) Facility Security Plan ....................................................................... 21  
  §164.310 (a)(2)(iii) Access Control and Validation Procedures ................................... 21  
  §164.310 (a)(2)(iv) Maintenance Records ................................................................... 22  
  §164.310 (b) Workstation Use .................................................................................... 22  
  §164.310 (c) Workstation Security ............................................................................. 23  
  §164.310 (d)(1) Device and Media Controls ................................................................. 23  
  §164.310 (d)(2)(i) Disposal ......................................................................................... 24  
  §164.310 (d)(2)(ii) Media Re-use .................................................................................. 25
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>§164.310 (d)(2)(iii)</td>
<td>Accountability</td>
</tr>
<tr>
<td>§164.310 (d)(2)(iv)</td>
<td>Data Backup and Storage</td>
</tr>
<tr>
<td><strong>§164.312 Technical Safeguards</strong></td>
<td></td>
</tr>
<tr>
<td>§164.312 (a)(1)</td>
<td>Access Control</td>
</tr>
<tr>
<td>§164.312 (a)(2)(i)</td>
<td>Unique User Identification</td>
</tr>
<tr>
<td>§164.312 (a)(2)(ii)</td>
<td>Emergency Access Procedure</td>
</tr>
<tr>
<td>§164.312 (a)(2)(iii)</td>
<td>Automatic Logoff</td>
</tr>
<tr>
<td>§164.312 (a)(2)(iv)</td>
<td>Encryption and Decryption</td>
</tr>
<tr>
<td>§164.312 (b)</td>
<td>Audit Controls</td>
</tr>
<tr>
<td>§164.312 (c)(1)</td>
<td>Integrity</td>
</tr>
<tr>
<td>§164.312 (c)(2)</td>
<td>Mechanism to Authenticate Electronic Protected Health Information</td>
</tr>
<tr>
<td>§164.312 (d)</td>
<td>Person or Entity Authentication</td>
</tr>
<tr>
<td>§164.312 (e)(1)</td>
<td>Transmission Security</td>
</tr>
<tr>
<td>§164.312 (e)(2)(i)</td>
<td>Integrity Controls</td>
</tr>
<tr>
<td>§164.312 (e)(2)(ii)</td>
<td>Encryption</td>
</tr>
</tbody>
</table>
Introduction

Purpose of this Document
This document is provided by UNCG’s division of Information Technology Services (ITS) to assist University entities to comply with the requirements of the HIPAA Security Rule. The sections of the Security Rule titled Administrative, Physical, and Technical Safeguards contain a large number of technology-based standards and specifications. The purpose of this document is to explain these requirements in non-technical language and describe methods that will help meet those requirements within the context of the UNCG network and services provided by Information Technology Services (ITS).

Please note that this document is not a mandate or statement of policy (though it will at times refer to University policy). Entities are free to substitute an equivalent alternative for any or all recommendations in this document; however, such substitutions must be developed, implemented and supported by the Covered Entity itself.

Important Terms
The following terms and abbreviations are used frequently in this document:

- **HIPAA Security Rule** – The section of HIPAA related to the security of electronic PHI; HIPAA Security Rule regulations are enumerated in the Code of Federal Regulations, Title 45 Section 164 Subpart C, and entitled “Security Standards for the Protection of Electronic Protected Health Information.”
- **PHI** – Protected Health Information. Individually identifiable health information. When such information is transmitted or maintained electronically this document refers to it as **ePHI**.
- **Hybrid Entity** – An entity which is comprised of units whose business activities include HIPAA-covered and non-covered functions. UNCG is a Hybrid Entity.
- **Covered Entity** – an entity that is, as a UNCG unit providing health care services, subject to the HIPAA Security Rule. In this document this term is commonly used to refer collectively to an entity’s compliance efforts led by the Compliance Officer.
- **Business Associate** – an entity that performs work for or on behalf of a Covered Entity; this may be another UNCG unit or an external entity. If the Business Associate is part of the same Hybrid Entity as the Covered Entity a contractual agreement is not required.
- **Compliance Officer** – The individual within a Covered Entity or Business Associate with ultimate responsibility for the entity’s compliance as specified in the University’s **HIPAA COMPLIANCE POLICY**. The individual may also be referred to as a Security Officer. In this document the term is used when reference must be specifically made to the unit’s individual officer, rather than the unit’s compliance team or the entity as a whole. When referring to the general compliance efforts of an entity led by the Compliance Officer, this document uses the term Covered Entity.
Organization of this Document

This document is composed of four parts. The first is this introduction which provides an overview and presents certain concepts that will be used in the remainder of the document. Following the introduction are sections devoted to Administrative, Physical and Technical safeguards of the HIPAA Security Rule, which appear as sections §164.308, §164.310, and §164.312 in Title 45 Code of Federal Regulation §164 Subpart C “Security Standards for the Protection of Electronic Protected Health Information.” Within the three “Safeguards” sections, each standard and implementation specification is given its own heading under which the text from the Security Rule is quoted, followed by explanatory text and often references to more detailed documentation on the subject.

Please note that reference numbers and quotes in this document are provided to assist the reader in referencing the proper section of §164 Subpart C from the Code of Federal Regulations (CFR). This document is intended to be used as a supplemental resource by UNCG entities subject to and, not a substitute for, the CFR or for professional legal advice.

Standards and Implementation Specifications

This document focuses on the sections of the Security Rule titled Administrative, Physical, and Technical Safeguards. These parts of the security rule typically use the following structure: a heading, referred to as “Standard,” which may be followed by one or more “Implementation specifications.” Standards are the requirements of HIPAA with which a Covered Entity must comply. Implementation specifications are subordinate to the standards and identify specific ways a Covered Entity may meet the overall requirements described in the standard. It is important to note that meeting the implementation specifications of a standard is not necessarily sufficient to comply fully with the standard. Put another way, implementation specifications describe methods for responding to the specification, but there may be additional methods developed and implemented by the Covered Entity to fully comply with the standard.

Implementation specifications are classified as either “required” or “addressable” – noted parenthetically in the description. Required implementation specifications must be implemented as described. Addressable implementation specifications, as described fully in §164.306 (d)(3) of the Security Rule, permit a Covered Entity to determine if the addressable implementation specification is appropriate for the Covered Entity. If it is appropriate then the specification should be implemented as described. If it is not appropriate, the Covered Entity must document why this is the case and implement an equivalent alternative. If the issue an addressable implementation specification addresses is not applicable to a particular Covered Entity then the entity should document why this is the case.

Covered Entities and Business Associates

There are two groups of University entities subject to HIPAA: healthcare providers who generate and store protected health information (PHI) and entities that receive PHI from another source. The former are referred to as Covered Entities; an example would be Student Health Services. The latter are referred to as Business Associates; an example
would be a researcher who obtains health data from a hospital in connection with work the researcher will perform for or in conjunction with the hospital.

For clarity’s sake, this document is written for a presumed audience of Covered Entities and their Compliance Officers. However, much of the information contained herein is equally applicable to Business Associates, especially those sections with specific technology-based recommendations for the security of ePHI.

When an entity (e.g., a faculty researcher) performs work for or on behalf of a Covered Entity, that entity must enter into a Business Associate agreement with the Covered Entity. As part of that agreement, it is possible that the Covered Entity will provide a list of security requirements it expects the Business Associate to meet. Rather than implementing such requirements on an ad-hoc basis, it is strongly recommended that the Business Associate negotiate with the Covered Entity to accept the security standards implemented by the University as described in this document in lieu of the Covered Entity’s unique requirements.

It is worth mentioning that the least complex method for a potential Business Associate to address HIPAA security concerns is to request de-identified PHI and thus avoid HIPAA compliance with respect to that information and the restrictions of the Security Rule. If such de-identified data is acceptable for the needs of the potential Business Associate, then it is highly recommended that the entity use such data in place of PHI.

Additional information for researchers wishing to use PHI is available from the Institutional Review Board, part of the University’s Office of Research Compliance at http://www.uncg.edu/orc/irb.htm

§164.308 Administrative Safeguards

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

*Implement policies and procedures to prevent, detect, contain, and correct security violations.*

The following four elements (Risk Analysis, Risk Management, Sanction Policy, and Information System Activity Review) describe a Covered Entity’s overall obligation to plan and implement a strategy for securing ePHI.

Many requirements in the remainder of the security rule will address (singly or collectively) parts of these four elements; however, the Covered Entity must meet the overall intent of the security rule as described in this standard when developing policies and procedures. If a procedure is identified that improves the security and integrity of ePHI, then the Covered Entity should document and implement this procedure, even if there is not a specific implementation specification detailed in the security rule for this procedure.
§164.308 (a)(1)(ii)(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)

The first step in any security plan is to examine existing equipment, technology, policies and procedures related to the use of the data (in this case, ePHI) and identify potential threats to the security of this data. Note that the security rule does not limit the concept of “security” to confidentiality, that is, preventing an unauthorized person from assessing ePHI. It also includes integrity (protecting the data from accidental or intentional destruction or unauthorized modification) and availability (accessibility at all times and under all circumstances).

Covered Entities are encouraged to research and develop risk analysis methodologies which best fit the operation of their organization. National professional organizations in a Covered Entity’s field are often a good starting resource for risk analysis tools and methodologies. A Covered Entity can consult with UNCG’s HIPAA Privacy and Security Officers for additional information.

It is important to note that risk analysis is a continuing process that must become part of a Covered Entity’s ongoing security and compliance efforts.

§164.308 (a)(1)(ii)(B) Risk Management

Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306 (Security Standards: General Requirements). (Required)

After identifying potential risks, a Covered Entity must implement a management process for evaluating and responding to each risk to comply with the security standard general requirements. Many of the requirements of the security rule will assist in limiting certain risks; however, these requirements alone will not serve to limit all potential risks for a Covered Entity.

While it is beyond the scope of this document to provide a detailed risk management strategy, a general approach might involve taking one of the following actions regarding an activity or operation with an identified risk:

- Determine that the probability of an identified risk occurring is so low that the risk may be classified as acceptable. Covered Entities should be cautious in classifying a risk as acceptable and should be prepared to support this assessment.
- Manage the risk with appropriate technological security measures, policies and procedures as described in this document and consistent with University data security policies.
- Avoid the risk by developing an alternative method of performing the activity or operation.
• If an alternative method cannot be determined, take actions to limit or reduce the risk inherent in the activity or operation.

Note that a Covered Entity should document each response to a potential risk as part of its ongoing risk management efforts.

§164.308 (a)(1)(ii)(C) Sanction Policy

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

The third component of the security management process is a documented sanction policy. This policy acts to preserve the integrity of a Covered Entity’s policies by responding to employee actions that violate these policies. Developing such procedures is a matter internal to the Covered Entity within the parameters set forth in University policy, Federal and State law; however, there may be technology-based ramifications to certain disciplinary actions, as noted below.

The sanction policy may include a reduction of an employee’s access to ePHI or other disciplinary action. For ePHI stored in the Covered Entity’s network ePHI storage space, the Compliance Officer or a delegate will have discretion to change the access permissions for each user as addressed in §164.308 (a)(3)(ii)(B), Workforce Clearance Procedure. The methods for doing so are discussed under §164.308 (a)(4)(ii)(C), Access Establishment and Modification.

If a particular sanction incident will result in termination of the employee, the Compliance Officer should also review the recommendations of §164.308 (a)(3)(ii)(C), Termination Procedures.

§164.308 (a)(1)(ii)(D) Information System Activity Review

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

An information system is something that exists for the collection, processing, storage, transmission and analysis of data. Generally, this refers to computer systems (hardware and software), the users of those systems and the procedures by which those users operate the system, but may be used to refer to other, non-electronic, entities as well. Covered Entities should identify what systems and processes within their organization qualify and determine appropriate methods to review the activity on these systems.

It is recommended that Compliance Officers set a formal schedule for reviewing system activity for those systems used by the entity to work with ePHI. The frequency of the review must be determined by the Compliance Officers based on
internal procedures. It is recommended, however, that such a review take place on a frequent basis as it permits the discovery of incidents in a timely manner, prevents the volume of activity to be reviewed from becoming unmanageable, and mitigates potential harm in the event of a security breach or non-compliant activity.

A review process should include, but is not limited to, the following actions:

- Access and modification of ePHI stored in the ITS shared file space should be reviewed using appropriate tools. Contact the UNCG Security Officer for information about current tools and techniques.
- If a Covered Entity utilizes a database application for storing and manipulating ePHI, the log files of this application should be reviewed as a part of the Information System Activity Review. If a covered entity is considering purchase of such an application, ITS recommends that the logging capabilities of the software be carefully evaluated prior to purchase.
- The current status of any security incidents during the review period should be noted and followed up on if necessary (e.g., if a workstation became infected with a virus, was the workstation wiped and reimaged according to standard procedures?)

§164.308 (a)(2) Assigned Security Responsibility

_Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity._

The University’s [HIPAA Compliance Policy](#) requires each entity subject to HIPAA to appoint a Compliance Officer. For the purposes of this document, the Compliance Officer is considered to be the individual with ultimate administrative responsibility for the information systems used to store ePHI in that unit.

In some cases, the Compliance Officer may delegate certain technology-based responsibilities (e.g., the administration of permissions for the Covered Entity’s network ePHI storage space) to another individual. These delegations of authority should be documented. Additionally, the annual report to the University’s HIPAA Security Compliance Officer should include the names of those individuals with administrative rights to the information systems containing ePHI.

The Compliance Officer (or his or her delegate) will have a number of technology-based authorities such as administrative rights over the network ePHI storage space and administrator access to workstations within the Covered Entity. Covered Entities are encouraged to document these technology-based rights and permissions to ensure a smooth transition of authority if and when the role is passed to another employee.
§164.308 (a)(3)(i) Workforce Security

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) [Information Access Management] 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.

This requirement, and the following three specifications (Authorization/Supervision, Workforce Clearance, Termination) dictate the requirements for granting and limiting access to ePHI by employees of a Covered Entity. A Covered Entity is expected to develop and document procedures that specify who is able to access ePHI and how this access is granted.

This section, Workforce Security, is closely associated with the following section, Information Access Management. This section deals with the overall policy by which access to ePHI will be controlled and the following section is concerned with the mechanism of how these controls are managed.

From a technical standpoint, this control will be implemented by storing ePHI where it may only be accessed by an authentication process (e.g., a username and password) and by implementing a mechanism for limiting access to ePHI to authorized accounts. It is important to note that this mechanism emphasizes the role of account integrity. Covered Entities are encouraged to create documented policies concerning topics such as sharing account information and eliminate ePHI access via multiple-user shared accounts.

Though a detailed discussion belongs under the following section, Information Access Management, it may be helpful to summarize some of that discussion here. ITS anticipates that account-based ePHI access control will typically occur in two ways. Firstly, documents containing ePHI will be stored exclusively in network file space designated for ePHI storage for which there will be an access and permissions list maintained by the Compliance Officer (see §164.308 (a)(4)(i) Information Access Management and §164.308 (a)(4)(ii)(B) Access Authorization for more details). Secondly, the Covered Entity may use some sort of ePHI storage application or database purchased and supported by the Covered Entity. This application should provide username-based access control also managed by the Compliance Officer.

If ePHI must be stored in a manner different from those described here, the Covered Entity must develop procedures for limiting access to this ePHI to authorized staff.

§164.308 (a)(3)(ii)(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)
Covered Entities should document procedures for how access to ePHI is granted and who within the entity is authorized to modify an employee’s rights to access ePHI.

It is appropriate and expected that authorized managers will have access to computing resources (such as individual workstations) within their department for the purposes of ensuring compliance. It is recommended that authorized managers perform inspections of such resources on a periodic schedule. This specification provides one place where documenting this access and employees’ expectations of privacy would be appropriate.

If maintenance on information systems used to store or access ePHI must be performed, HIPAA-trained ITS support staff are available upon request. Additionally, administrative access to the ITS-managed servers containing ePHI, as well as access to the backup media from these servers, is limited to ITS staff trained on HIPAA security.

HIPAA introductory information is available on the UNCG HIPAA “landing page” at http://provost.uncg.edu/publications/general/hipaa.aspx. Additional training is provided to members of Covered Entities through a general HIPAA online course through Blackboard, and through training delivered by each Covered Entity.

§164.308 (a)(3)(ii)(B) Workforce Clearance Procedures

*Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate. (Addressable)*

It is expected that different employees will have different access rights to ePHI based upon the role they perform.

A rule of thumb for data security is to grant each user the very minimum access required for the performance of their duties. For example, if an employee needs to read a document, but should not modify it, that user should not be provided rights to change and save the document, only view it.

Rather than documenting access rights to ePHI on an employee by employee basis, Covered Entities may find it helpful to define a number of user groups with a particular set of access permissions and then manage the permissions of each employee by associating them with a particular group. In the case of a department’s central ITS-provided ePHI storage space, folders within the network file space should be organized so that ePHI used by specific groups is stored together; the administrator may then manage the permissions for each folder, rather than each individual file.
Once a structure for organizing ePHI is determined (with an associated set of permissions), each employee should be assigned to a particular ePHI access group based on job classification, work unit or by other documented method. This assignment defines an appropriate level of access for that employee.

The central ITS-provided file system allows for granular control of what a user can and cannot do with each file. If a Covered Entity is researching the purchase of an ePHI management tool or database, careful consideration should be given to the level of access control it offers as part of the purchase decision. Such software should provide equivalent capabilities for access control and activity review as the central ITS-provided file system (Contact the UNCG HIPAA Security Officer for information) provides for files stored in that system.

Finally, it is understood that all employees must successfully complete training and demonstrate understanding of HIPAA regulations and Covered Entity policies and procedures as a pre-requisite to access authorization.

§164.308 (a)(3)(ii)(C) Termination Procedures

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 [Workforce Clearance Procedure].

(Addressable)

When an individual with access to ePHI leaves the department or University, the Compliance Officer must notify the ITS Technology Service Center (6-tech) of the change in status so that the proper action may be taken with the individual’s accounts.

If the individual is leaving the University, then the Compliance Officer should fill out the UNCG Expire and Delete Accounts Request Form found at http://accounts.uncg.edu. The form asks for an expiration date and a deletion date for the account. After the expiration date, the account may no longer be used to access campus resources. All data will need to be moved to an active account prior to the deletion date in accordance with record retention and disposition schedules, any litigation holds, and further needs to access the data in the unit. After the deletion date, all data contained in the account’s network space will be deleted.

If an individual is leaving the department but not the University, the Compliance Officer should submit the UNCG Department Change Form, also found at http://accounts.uncg.edu.

When possible, these forms should be submitted in advance of the individual’s change in status. If an employee’s change in status is unexpected (e.g., termination or resignation without notice), the Compliance Officer should
immediately contact the ITS Technology Service Center (6-tech) and request deactivation of that user’s accounts.

In both cases described above, the Compliance Officer will need to modify the permissions to the Covered Entity’s network ePHI storage space as described in §164.308 (a)(4)(ii)(C), Access Establishment and Modification. The Compliance Officer will need to remove the individual’s account from the permissions list for the department’s ePHI folder.

If a Covered Entity operates an information system used to store or access ePHI which authenticates independently from the centralized University authentication service (e.g. an accounting program bought and managed by the Covered Entity), then the Covered Entity should have policies in place to modify access to these systems as part of termination procedures.

§164.308 (a)(4)(i) Information Access Management

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.

As mentioned in §164.308 (a)(3)(i) Workforce Security, this requirement and its subheadings specify the mechanism by which the access controls described in Workforce Security are implemented. It is assumed that Covered Entities will use designated space on the central ITS-provided file servers to store documents containing ePHI and the discussion in this section is written with this scenario in mind.

It is recommended that, wherever practical, Covered Entities isolate data containing ePHI from other data. This should assist in the management of the access security for the ePHI as well as the review of system activity, as described under §164.308 (a)(1)(ii)(D) Information System Activity Review.

Covered Entities may also use a database or other application to store and manage ePHI. Information access management processes for these applications will need to be developed, training conducted for, and enforced by the Covered Entity.

§164.308 (a)(4)(ii)(A) Isolating Healthcare Clearinghouse functions

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)
This standard only applies to entities which contain a healthcare clearinghouse as part of their organization. At the time of this writing, there is no such organization at UNCG.

§164.308 (a)(4)(ii)(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)

This implementation specification is closely related with the following specification, Access Establishment and Modification. This specification requires that a process or mechanism for granting access to ePHI be defined whereas the following specification involves how these processes are applied to individual employees.

As has been discussed, ITS recommends that all ePHI be stored exclusively within a dedicated folder tree on the central ITS-provided file servers (and/or within a database or application for managing ePHI administered by the Covered Entity). In this scenario, access authorization is granted by the use of a username and password for which the associated account has been granted a certain degree of access to ePHI.

For the ePHI folder on the central ITS-provided file servers, the Covered Entity Compliance Officer (or a delegate) will be granted administrative rights to the folder which will allow them to manage who may access the files within this folder as well as the degree of access each user has (e.g., whether a user can read a document or modify it, etc.). A link is provided below to detailed documentation for performing these functions.

If a Covered Entity uses some sort of database or application for storing ePHI, documentation on how the application manages access authorization should be prepared.

§164.308 (a)(4)(ii)(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)

The previous standard (Access Authorization) requires that a method for access authorization be defined. This closely related standard requires that processes for managing this method with individual employees be defined.
As discussed in §164.308 (a)(3)(ii)(B) Workforce Clearance Procedures, there may be groups of employees which share similar rights to access a department’s ePHI. These groups might divide along job classification lines or by teams within the department. In any case, the access establishment and modification procedures may be tied to an employee joining or leaving one of these groups (e.g., when an employee is hired, promoted or terminated, the Compliance Officer will review the access authorization of the employee based on the procedures developed to meet this requirement).

The documentation referred to in §164.308 (a)(4)(ii)(B), Access Authorization, provides the Compliance Officer with the instructions and recommendations for creating and organizing the Covered Entity’s PHI network storage space.

§164.308 (a)(5)(i) Security Awareness and Training

*Implement a security awareness and training program for all members of its workforce (including management).*

The most significant threat to the security of electronic data is often those users authorized to access that data. By intent or accident, an authorized user is far more likely to compromise a carefully implemented security plan than an outside entity. Because of this, a key part of any security plan must be the establishment of a culture of security awareness within an organization with ongoing security training and oversight.

This standard has four implementation specifications associated with it: Security Reminders, Protection from Malicious Software, Log-in Monitoring, and Password Management.

§164.308 (a)(5)(ii)(A) Security Reminders

*Periodic security updates. (Addressable)*

It is important that Covered Entities remain up-to-date with the latest potential security threats to the entity’s ePHI. This effort may take many forms, depending on the sort of risks identified in §164.308 (a)(1)(ii)(A) Risk Analysis and §164.308 (a)(1)(ii)(B) Risk Management.

Typically, there will be two steps in a Covered Entity’s security reminder process. The Compliance Officer (or a delegate) will need to maintain an awareness of developing security issues for the purpose of proactively protecting the ePHI. For the purpose of ongoing security awareness and training, this individual will then need to organize and distribute the information into a form appropriate for the rest of the staff.

There are a number of resources a Compliance Officer may use to remain informed. Mailing lists (also called listservs) offer timely updates on a number of subjects, including information security. There are a number of websites
dedicated to providing security news and information. It is also important to monitor the web sites of any software vendors utilized by the Covered Entity for the latest security updates concerning those software packages. See the UNCG HIPAA “landing page” at http://provost.uncg.edu/publications/general/hipaa.aspx for current information.

§164.308 (a)(5)(ii)(B) Protection from Malicious Software

Procedures for guarding against, detecting, and reporting malicious software. (Addressable)

Malicious software includes any program that interferes with the operation or security of a computer, including viruses, trojans, worms, spyware, etc. The recommended strategy for minimizing these threats involves reducing a computer’s potential exposure to these threats and blocking the common methods (or vectors) of infection. The Covered Entity may contact the ITS Security Officer to arrange a consultation on this subject.

§164.308 (a)(5)(ii)(C) Log-in Monitoring

Procedures for monitoring log-in attempts and reporting discrepancies. (Addressable)

A key advantage of using account-based access control for ePHI (e.g., requiring a username and password to access ePHI) is that such systems make it possible for an administrator to review who is attempting to access the data and whether they are successful.

This implementation specification is related to the requirements of §164.308 (a)(1)(ii)(D), Information System Activity Review, and in practice may occur as part of the same process. This specification is more focused than the earlier requirement, however. It is concerned with identifying attempts to circumvent the access controls first mentioned in §164.308 (a)(3)(i), Workforce Security. This may be accomplished by reviewing the activity logs of the information systems used by the Covered Entity and looking for suspicious login activity.

Such suspicious activity includes, but is not limited to:

• Repeated failed login attempts by a user in a short time frame – This may indicate a person or program is attempting to guess the account’s password.

• An account being logged in from multiple locations concurrently – This may indicate someone has gained access to another user’s account. It may also mean the user has failed to log off from one location before moving to another.
• Login attempts outside of normal operating hours – If it is expected that access to ePHI will occur only during business hours, access at unusual times should be investigated.

For ePHI stored in the designated central ITS-provided file space, contact the UNCG HIPAA Security Officer for information about tools to perform log-in monitoring. If a Covered Entity uses another database or software package for managing ePHI, the entity must develop procedures for reviewing activity on those systems.

As an additional help in facilitating the tracking of user activity and access attempts, it is recommended that workstations being used to work with ePHI be configured to prohibit the user from logging into the local workstation. Though ITS will provide tools to assist the Covered Entity with auditing tasks for information stored in central ITS-provided file space, it is the responsibility of the Compliance Officer to review the activity on information systems used to store that entity’s ePHI.

§164.308 (a)(5)(ii)(D) Password Management

_Procedures for creating, changing, and safeguarding passwords._
(Addressable)

An extremely important part of an account-based access authorization plan is for authorized users to create strong passwords. A strong password is one which is difficult for an attacker to discover though knowledge of the user or through a brute force attack using a password cracking utility. Many users choose passwords based on how convenient the password is to remember, not how strong the password is, so it is important that Covered Entities train their authorized users on the importance of choosing a password that will maintain the security of the ePHI and support this training with policies.

§164.308 (a)(6)(i) Security Incident Procedures and §164.308 (a)(6)(ii) Response and Reporting

_Implement policies and procedures to address security incidents._

Though every attempt should be made to anticipate and prevent security incidents from occurring, it is reasonable to expect that such incidents may occur. This standard requires that Covered Entities put processes in place for responding to these events.

The definition of a security incident under the HIPAA Security Rule is found in §164.304: “[A] security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.” Note that an attempt to
compromise the security of ePHI qualifies as a security incident – the attempt need not be successful.

Please see the Personal Information Security Breach Notification Policy at http://www.uncg.edu/cha/policy_manual/security_breach_notification/ for more information on your responsibilities and the process to be followed.

In all cases, the Covered Entity should document and retain security incident reports and reviews according to the standards of the University’s HIPAA Compliance Policy. Also note that this policy requires that Compliance Officers provide periodic reporting to the University’s HIPAA Security and Privacy Officers.

§164.308 (a)(7)(i) Contingency (Business Continuity) Plan

Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

As mentioned in §164.308 (a)(1)(ii)(A), Risk Analysis, information security involves not only confidentiality, but integrity and availability as well. This standard and its four implementation specifications help address the integrity and availability of ePHI during a range of operational conditions outside of the norm.

It is required by policy (Security of Networks and Networked Data, found at http://www.uncg.edu/cha/policy_manual/network_security/) that ePHI not be stored locally on a department’s computers but instead be stored on the University’s central ITS-provided file servers located in the campus data center(s). A very important reason for this is the protection this offers ePHI during a disaster or other contingency. The document titled “UNCG’s Information Technology Services’s Contingency Planning and Disaster Recovery” details how the University will respond to such events and the schedule by which critical computing resources will be restored.

If a Covered Entity’s ePHI is stored in such a way as to be covered by the “UNCG’s Information Technology Services’s Contingency Planning and Disaster Recovery” plan, the process planning required by this standard mostly involves protecting those resources directly under the control of the Covered Entity.

Assuming the data itself is stored outside of the Covered Entity’s facility (i.e., on the central ITS-provided servers), the primary concern during an emergency (after the safety of personnel) is terminating the access to the ePHI from local workstations. If the situation permits, employees should close out of all applications storing ePHI and log out of the network prior to exiting the facility.
While the Covered Entity is in emergency operation mode, the entity should have plans in place for accessing critical data from an alternate site arranged in advance with ITS. Note that even if an entity ceases most operations during an emergency, some data stored by the entity (e.g., health records) may need to be accessible.

Covered Entities should also have a plan for the post-emergency period and procedures for restoring operations. It is also a good idea to inventory the entity’s computing equipment to ensure that it all can be accounted for.

Copies of a Covered Entity’s contingency (Business Continuity) plans should be kept in a secure, off-site location to ensure access to these procedures during a disaster scenario.

§164.308 (a)(7)(ii)(A) Data Backup Plan

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

An important advantage of storing ePHI on the central ITS-provided file servers is that it allows a Covered Entity to take advantage of the robust data backup processes ITS has implemented to protect data on University servers.

ITS backup procedures operate under the University’s Computer Systems Backup Procedure, according to the schedule specified in that Procedure.

It is important for Covered Entities to note the implications of the University’s backup procedure and the various Records Management data retention requirements (see http://www.uncg.edu/cha/policy_manual/electronic_records/) to which ePHI may be subject, namely, that the backups do not serve as long-term storage for data retention purposes. What this means is that data must be maintained on the server for the longest of the length of time required by the Covered Entity or UNCG policies (including record retention and disposition schedules) or law (unless an alternative long-term retention procedure is put in place).

The email is not classified as a data store. Covered Entities should not store ePHI in an email form. Also note that in the discussion of §164.312 (e)(1), Transmission Security, email is not recommended for the transmission of ePHI.

§164.308 (a)(7)(ii)(B) Disaster Recovery Plan

Establish (and implement as needed) procedures to restore any loss of data. (Required)
For disasters that affect the entire University, the recovery of ePHI stored on University servers is managed through “UNCG’s Information Technology Services’s Contingency Planning and Disaster Recovery” plan.

If an event is localized to the Covered Entity (e.g., accidental deletion of ePHI), data recovery can be initiated by contacting the ITS Technology Service Center (6-Tech). It is important for the Covered Entity to identify to the best of its ability the exact files or directories that must be restored. As noted in §164.308 (a)(7)(ii)(A), Data Backup Plan, ITS will be able to restore data as described in the Computer Systems Backup Procedure. Covered Entities must be able to recreate the data between the last backup and the event requiring a restoration of data.

§164.308 (a)(7)(ii)(C) Emergency Mode Operations 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)

For disasters that affect the entire University, the access to ePHI stored on University servers during “emergency mode” is managed through “UNCG’s Information Technology Services’s Contingency Planning and Disaster Recovery” plan.

If an event is localized to the Covered Entity then access to ePHI stored on University servers should be accessed according to a process pre-arranged with ITS. It is important to anticipate all applications required to access ePHI in addition to planning for hardware (workstations) to access the data. Identifying such critical applications is a component of §164.308 (a)(7)(ii)(E), Application and Data Criticality Analysis.

If certain resources (such as software needed to access ePHI) are not standard ITS-supported products or services, the Covered Entity will need to plan for restoring that resource themselves. For example, a backup copy of software purchased to manage patient billing should be kept in a secure off-site location as part of an Covered Entity’s contingency plan – even if the data is safely stored on the University’s servers, the software may be needed to access that data.

§164.308 (a)(7)(ii)(D) Testing and Revision Procedures

*Implement procedures for periodic testing and revision of contingency plans.* (Addressable)

“UNCG’s Information Technology Services’s Contingency Planning and Disaster Recovery” plan is revised on an annual basis and it is recommended that Covered Entities review their procedures on a similar schedule.
§164.308 (a)(7)(ii)(E) Application and Data Criticality Analysis

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

It is important for a Covered Entity to have a written specification of what technology resources are required for both normal and contingency operation. This specification would include things such as workstations, applications, and network data that must be accessed – any technology needed to operate the Covered Entity.

As noted in §164.308 (a)(7)(ii)(C), Emergency Mode Operations Plan, resources (such as software) not provided through ITS should be identified and provisions made for their restoration in the event of an emergency.

§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 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.

Information security is an ongoing process. In addition to the initial risk analysis and responding to security incidents as they arise, a Covered Entity is required by this standard to perform periodic reviews and revisions of their security procedures. The “subpart” referred to is the HIPAA Security Rule, as noted in the introduction, so this standard applies to all compliance efforts under that rule.

Such a review process should include, but is not limited to, the following:

- A review of security incidents, as described under §164.308 (a)(6)(i) Security Incident Procedures.
- The results of any contingency plan tests or actual emergency responses, as described under §164.308 (a)(7)(i) Contingency Plan.
- A review of any changes in the entity’s operating processes (e.g., staff organization or reporting) which may justify a revision in security procedures.
- A review of significant changes to the computing infrastructure (e.g., new software or a major upgrade in existing software) that might require an update to security procedures.
- A review of changes to the physical environment (e.g., new construction or a change of location) that could impact security procedures.

The frequency of the evaluation process must be determined by the Covered Entity; however, it is recommended that it take place on at least an annual basis. These evaluations should be made available to the University’s HIPAA Officers as described in the University’s HIPAA Compliance Policy.
§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. […]

When a Covered Entity wishes to let an external entity store, process or otherwise use its ePHI on behalf of the Covered Entity, the Covered Entity is required to enter into a Business Associate contract with that external entity. While it is beyond the scope of this document to provide a detailed discussion on Business Associate arrangements, in summary these contracts dictate how the external entity is expected to protect the ePHI through organizational and technology-based means specified by the Covered Entity.

It is important to note that the University as a whole is a Hybrid Entity subject to HIPAA, and thus units within the University are not required to enter into Business Associate agreements with each other (e.g., a Covered Entity does not need to have a Business Associate agreement with ITS to receive technical support).

§164.308 (b)(4) Written Contract or Other Arrangement

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) [Business Associate Contracts and Other Arrangements]. (Required)

Business Associate Agreements must be reviewed and approved prior to execution by the University’s HIPAA Privacy and Security Officers as well as University Counsel consistent with the UNCG’s Policy on Contract Review and Approval.

§164.310 Physical Safeguards

§164.310 (a)(1) Facility Access Controls

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.

Much of what has been discussed concerning the security of ePHI has involved using what could be broadly described as information systems to protect the data. Such protections are of limited use if the physical device containing that data is vulnerable. It is the protection of this hardware which is the focus of this section of the Security Rule.
As restricted data, as defined in the University’s Data Classification Policy, all ePHI must be stored on servers which physically reside in one of the ITS computing facilities. Access to these facilities is tightly controlled. Only a small number of authorized ITS technicians are permitted to enter the rooms and they do so under the supervision of a Technology Service Center Manager, one of whom is on duty at all times. If ePHI cannot be stored in compliance with the University’s Security of Networks And Networked Data Policy (e.g., on a local workstation), the Covered Entity Compliance Officer must request a written exception to that policy from the UNCG HIPAA Security Officer.

While this significantly reduces the threat posed by physical risks to the computing equipment operated by a Covered Entity, it does not eliminate it. An authorized individual might store ePHI on their workstation by accident or intent, contrary to departmental and University policy. If a workstation is left logged into a resource storing ePHI, someone might take advantage of this open access. Because of these and similar concerns, Covered Entities must develop and use procedures for protecting local computing resources.

This standard, Facility Access Controls, requires that a Covered Entity control physical access to its electronic information systems and the facilities in which they are housed. For most Covered Entities, this means access to the desktop computers used to work with ePHI as well as any electronic media containing ePHI.

The first step in developing these procedures is identifying which computing resources in a department might feasibly use to access, store, or otherwise interact with ePHI. Once these resources are identified, the Covered Entity can evaluate potential risks and address them.

This standard has four implementation specifications: Contingency Operations, Facility Security Plan, Access Control and Validation Procedures, and Maintenance Records.

§164.310 (a)(2)(i) 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)

This specification is related to §164.308 (a)(7)(i), Contingency Plan, but is distinct from that standard. The plan documents to what extent and how a Covered Entity operates in a contingency situation. This specification deals with how and for what reasons a Covered Entity will access their facility during an emergency. Covered Entities should plan for the possible loss of the facility and
all its contents as part of its contingency planning; however, in cases of partial damage to the facility, access and recovery may be possible.

If a Covered Entity’s ePHI is stored on ITS-managed servers, ITS staff will be able to access these servers on the entity’s behalf during contingency operations. The Covered Entity will need to establish a plan in advance with ITS to provide alternative computing resources to access ePHI as part of the Covered Entity’s §164.308 (a)(7)(ii)(C) Emergency Mode Operations Plan. For example, the entity might require a workstation in an alternative location if the entity’s normal facilities are unavailable.

A Covered Entity should document and provide the University’s HIPAA Security Compliance Officer with a list of computing resources required by that entity’s contingency operations plan. Such a list should include specific network resources, such as central ITS-provided file space containing ePHI, to which access is required. Additionally, the manner in which these resources will be accessed should be specified.

The University’s capacity to support operations during an emergency is limited. Operational needs of Covered Entities during such periods must be balanced against other critical University functions. Covered Entities are asked to carefully consider what resources are absolutely necessary when developing their contingency plans.

§164.310 (a)(2)(ii) Facility Security Plan

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

A Covered Entity should implement procedures for securing locations where ePHI is used, both during normal operation and outside of normal business hours. Rooms containing computers on which ePHI is access should be locked when not in use. Windows and doors in the facility should be checked for proper operation and resistance to tampering. Removal of any equipment from the facility should be performed according to set procedures, including the verification of identification.

§164.310 (a)(2)(iii) 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)

This standard is primarily concerned with the access of individuals to and within the facility housing the Covered Entity and thus not within the scope of this document.
However, the specification does contain the language: “control of access to software programs for testing and revision.” A covered example would be if a covered entity receives remote support from a third party for an ePHI record-keeping application. In such case, the Covered Entity must document the conditions under which the third party may access the software for troubleshooting and updates.

Clients should also feel free to call the ITS Technology Service Center (6-Tech) to verify the identity of ITS personnel working at their facility.

§164.310 (a)(2)(iv) 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)*

As stated, a Covered Entity must log all repairs and modifications to the physical components of the facility.

If work is performed on a Covered Entity’s computing hardware by ITS staff, then a record of the work is maintained in ITS’s ticket-tracking software and is available on request.

§164.310 (b) 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 that can access electronic protected health information.*

All users of campus computing resources are subject to the University’s Acceptable Use of Computing and Electronic Resources Policy and it is suggested that Covered Entities reference that document as a starting point for defining their internal policies regarding workstation use.

Compliance Officers may wish to consider adding some or all of the following restrictions to their internal documentation concerning workstation use. Where possible, technical safeguards enforcing these restrictions are described elsewhere in this document; however, ITS recommends that these safeguards are supplemented with policies specifying appropriate use of workstations used to access ePHI.

Such a workstation use policy might include, but would not be limited to, the following:

- **ePHI may not be stored locally** – ePHI should not be stored on the hard drive of the local workstation or on any removable media or mobile device. As required by the University’s Security of Networks and Networked Data
Policy, restricted data must reside on “ITS network storage facilities.” ePHI should be exclusively stored on those network resources designated by the Compliance Officer.

- **Users may not install software** – To prevent the introduction of malicious software or compromising the operation of the workstation, users should be prohibited from installing any software on workstations used to access or manipulate ePHI. (§164.308 (a)(5)(ii)(b), Protection from Malicious Software)

- **Users may not modify the configuration of the workstation** – If a workstation has been specially configured for use with ePHI, the user should not be permitted to change or circumvent these settings.

- **ePHI may only be accessed from specified workstations** – Typically, certain workstations will have been secured, physically or through information systems, for use with ePHI. Employees should not attempt to access ePHI from other locations.

- **Unattended workstations must be locked** – When a user must leave the workstation unattended, they must lock out access to the workstation. (This is described in §164.312 (a)(2)(iii), Automatic Logoff.)

- **Unused workstations should be powered off** – Workstations which are not in use (e.g. outside of working hours) should be powered off to reduce their vulnerability to remote attacks.

- **Report suspicious activity** – If a workstation does not appear to be performing normally, this should be reported to the appropriate technical staff in a timely manner.

---

### §164.310 (c) Workstation Security

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

ITS recommends that workstations used to work with ePHI are secured against theft, either by keeping them in a controlled access area (e.g. a locked room) or by using a cable lock to secure the computer to a desk.

Additionally, it may be appropriate to position monitors or install screen filters to prevent unauthorized persons from viewing ePHI on the screen.

### §164.310 (d)(1) Device and Media Controls

*Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.*

The first step in a device and media control plan is a careful inventory of all such items that store or use ePHI within the Covered Entity’s facility. This will also be useful in performing the initial §164.308 (a)(1)(ii)(A) Risk Analysis and in developing the entity’s §164.308 (a)(7)(i) Contingency Plan. Such an inventory
should include both a description and location of the item in question as well as the employee assigned to the equipment, if appropriate.

It is recommended that all computing hardware relocations and installations be performed by ITS technicians according to ITS procedures. If a Covered Entity has internal technical support staff then procedures used by this staff should be documented.

It is required by policy (Security of Networks and Networked Data, found at http://www.uncg.edu/cha/policy_manual/network_security/) that unencrypted ePHI not be stored on removable media (floppy disks, CD-ROMs, USB flash drives, etc.), on mobile devices (laptops, PDAs, etc.), or on local hard drives because of the increased potential for loss or theft. It is expected that as part of an entity’s initial compliance efforts data will be discovered which is stored inappropriately on local workstations and removable media. This data should be transferred to a secure location, such as the designated ePHI storage space on the network, and the original media securely wiped, as discussed in §164.310 (d)(2)(i) Disposal.

If ePHI must be temporarily stored on portable media, the information should be encrypted by methods equivalent to those described in §164.312 (a)(2)(iv), Encryption and Decryption.

This specification has four implementation specifications: Disposal, Media re-use, Accountability, Data backup and storage.

**§164.310 (d)(2)(i) 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)*

Deleting a file from storage media using the operating system is not sufficient to ensure the data it contained is irrecoverable. However, methods do exist which permit data stored on media to be securely destroyed. Typically this will be performed prior to decommissioning or reassigning a workstation, or if removable media has been used temporarily to store ePHI. Even if the Covered Entity has procedures specifying that ePHI not be stored on a workstation, the possibility for ePHI to accidentally end up on the hard drive is significant enough to warrant securely wiping the drive.

Data stored on magnetic media (e.g., hard drives, floppy or zip disks) may be securely destroyed using software tools. These tools work by overwriting the section of the media containing the file with random information until traces of the original file are undetectable.
The methods used to securely wipe data on magnetic media will not work on optical media (e.g., a CD-ROM or DVD). Optical media must be physically destroyed. Shredding machines which handle CD-ROMs, as well as paper, are available and IT recommends using such a device to safely destroy optical media.

USB flash drives present a challenge to a user attempting to securely destroy data contained on the device. Though treating the device in the same manner as magnetic media appears to be the most effective method, this approach is less certain in its results than it is with magnetic media. Physical destruction is also an option. As such, it is not recommended that such devices be used to store ePHI.

ITS recommends that workstations designated for surplus or for reassignment be processed by ITS technicians to ensure the secure erasure of all data on the hard drives.

§164.310 (d)(2)(ii) 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)*

If media has been used or has been suspected of having been used to store ePHI, the processes described in §164.310 (d)(2)(i) Disposal may be used to prepare the media for reuse (at least in the case of magnetic media – optical media must be destroyed).

This requirement can apply to both removable media and the drives within the workstations themselves.

It is recommended that workstations being decommissioned or reassigned be processed by ITS technicians to ensure the secure destruction of all data from the workstation.

§164.310 (d)(2)(iii) Accountability

*Maintain a record of the movements of hardware and electronic media and any person responsible therefore. (Addressable)*

Once an inventory of hardware and media is performed (as discussed in §164.310 (d)(1) Device and Media Controls), it is important that this inventory be maintained by the Covered Entity.

If ITS staff must perform work on computers used with ePHI, it is preferred that the work take place at the equipment’s normal location, as this location will have been secured as part of the Covered Entity’s operating procedures.
As an additional resource, requests made to ITS for the installation, removal and reassignment of computers are documented in ITS’s ticket tracking software.

Storing ePHI on removable media or mobile devices should be avoided, as this is contraindicated by UNCG policy. However, if ePHI is transported via mobile computing device (e.g. a laptop) or on removable media (e.g. a CD-ROM), the Covered Entity should maintain a record of the existence, whereabouts and ultimate disposition of these items.

§164.310 (d)(2)(iv) Data Backup and Storage

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

As it is required by the Security of Networks and Networked Data Policy that no ePHI will be stored locally on media or computers managed by the Covered Entity, compliance with this standard should be straightforward. By virtue of being stored on ITS-managed servers, the ePHI is regularly backed up as described in §164.308 (a)(7)(ii)(A) Data Backup Plan.

However, it is still recommended that full backups be performed on any computing equipment undergoing relocation. This is standard procedure for equipment worked on by IT technicians and is suggested for support staff within the Covered Entity. Such backups should be made to a secure location and securely destroyed, according to §164.310 (d)(2)(i) Disposal, after the movement of equipment has been completed and the integrity of the data on the equipment has been confirmed.

The University’s Security of Networks and Networked Data Policy requires that all data classified as restricted must reside on ITS network resources (e.g., the dedicated ePHI storage space on central ITS-provided servers). If ePHI must be stored on a mobile device, such as a laptop, or on removable media, the Covered Entity must request a waiver to this policy from the UNCG HIPAA Security Officer, and such data shall only be stored in mobile form for the shortest possible duration as is necessary.

§164.312 Technical Safeguards

§164.312 (a)(1) Access Control

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)(4) [Information Access Management].
This section of the Security Rule deals with specific technology-based methods for securing ePHI, many of which have been mentioned in previous sections of this document.

This particular standard is concerned with how access to ePHI is limited to authorized persons. § 164.308 (a)(4), referred to in the quote, is Information Access Management. That standard requires that procedures for granting or limiting access to ePHI be defined. This standard requires that the technology to be used in implementing the information access management policies be described.

Two methods of storing ePHI have been presented in this document: storing ePHI in designated space on the central ITS-provided file servers and storing ePHI in a software package or database purchased and managed by the Covered Entity. In complying with this specification, a Covered Entity must define how employees will use these resources to store ePHI. For example, if a Covered Entity uses a software application for patient billing and maintains other ePHI records in electronic documents (e.g., Word or Excel files), under this standard the entity would specify that billing information must be stored in the billing application and all other ePHI must be stored in designated folders in central ITS-provided file space.

It is recommended that all Covered Entities prepare central ITS-provided file space for the storage of documents containing ePHI, even if the Covered Entity’s primary method of ePHI storage is in a dedicated application or database. This will allow the entity to include language to the effect that all ePHI without an otherwise specified storage location should be stored securely in the designated central ITS-provided file space.

This standard has four implementation specifications: Unique user identification, Emergency access procedure, Automatic logoff, Encryption and Decryption.

§164.312 (a)(2)(i) Unique User Identification

Assign a unique name and/or number for identifying and tracking user identity. (Required)

Whether a Covered Entity uses central ITS-provided file space or a dedicated application to store ePHI, access should be granted by a username/password combination; this username then acts as the unique identifier described in this implementation specification.

The specification states that this unique identifier is to be used to identify and track the user. For data stored on the central ITS-provided file servers, information about tools to track such access can be provided by the UNCG HIPAA Security Officer. If an entity is considering the purchase of ePHI management software, it should carefully review the software’s capability for
tracking user activity (i.e., does the software log what a user views and changes or does it simply log the user’s access to the software?).

It may be possible for some ePHI management tools to use the University’s authentication servers, minimizing the need for separate account management procedures. If the software supports LDAP authentication, the Covered Entity should contact the Technology Service Center (6-Tech) and request a consultation.

§164.312 (a)(2)(ii) Emergency Access Procedure

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

This specification requires that procedures for accessing ePHI during an emergency be put in place when that ePHI is stored according to the methods described in this rest of this standard. These processes should be developed in advance with the University’s HIPAA Security Compliance Officer as part of the §164.308 (a)(7)(i) Contingency Plan process.

§164.312 (a)(2)(iii) Automatic Logoff

*Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. (Addressable)*

Workstations used to work with ePHI must be configured to lock the user account after a period of inactivity. As mentioned in §164.310 (b) Workstation Use, it is recommended that Covered Entities institute a policy that workstations be manually locked by the user when they leave the workstation unattended.

§164.312 (a)(2)(iv) Encryption and Decryption

*Implement a mechanism to encrypt and decrypt electronic protected health information. (Addressable)*

This standard requires that a mechanism for encryption of ePHI be provided, but note that it does not require that all ePHI be encrypted. In general, as long as the ePHI remains on the central ITS-provided file servers, encryption is an additional security step that should not be necessary. If, however, ePHI must be removed from the central ITS-provided file servers, encryption is highly recommended.

It is worth noting here, however, that data which is effectively encrypted is not recoverable if the key or password is lost. Based on the requirements under §164.308 (a)(7)(i), Contingency Plan, ePHI must be protected from loss and accessible on demand. Because of this, a Covered Entity should only encrypt copies of records containing ePHI, and an unencrypted, primary, copy should be maintained on the central ITS-provided file servers. Changes to the ePHI record
should always be made to the unencrypted version of the file so that those changes remain accessible.

§164.312 (b) 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.

This standard is closely related to §164.308 (a)(1)(ii)(D) Information System Activity Review. That specification requires that a procedure for audits is established. This standard is where a Covered Entity describes the mechanism used to perform the audits.

If a Covered Entity uses a database or other software to manage ePHI, the entity must specify how activity on that system is to be audited. When researching the purchase of such software, the entity should review the activity auditing capabilities in candidate applications and may consult with the UNCG HIPAA Security Officer for assistance.

§164.312 (c)(1) Integrity

Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

As discussed in §164.308 (a)(1)(ii)(A) Risk Analysis, data security consists of integrity in addition to confidentiality and availability. Integrity, in this context, means that the data has not been accidentally or intentionally changed contrary to proper procedures.

For data stored in designated central ITS-provided file space, the first step in protecting ePHI from improper alteration or destruction is by making careful use of the file permissions system described in §164.308(a)(4)(ii)(C), Access Establishment and Modification. It is also possible to check files to see if they have been modified from a previously known correct state; this is described in the following section, §164.312 (c)(2) Mechanism to Authenticate Electronic Protected Health Information.

If a Covered Entity stores ePHI in some sort of management software or database, the integrity controls present in this software should be documented. When researching the purchase of such software, the entity should review the integrity controls present in candidate applications and may consult with the UNCG HIPAA Security Officer for assistance.

§164.312 (c)(2) 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.

A topic related to the integrity controls discussed in the previous standard is verifying if a record has been altered. For documents and other files (such as those stored in a central ITS-provided folder) the recommended method is to check the file against a digital
‘fingerprint’ of a known good version of the file called a hash, or signature. An explanation of this method is provided in another document. In summary, the Covered Entity periodically runs a program that creates a snapshot of all the files in the ePHI directory; if it is suspected that a file has been altered, the entity can verify the current version of the file with the snapshot and take appropriate action.

If a Covered Entity uses a database or other software to manage ePHI, the entity must use that application’s integrity verification functions to monitor whether modifications have occurred to that data. A robust ePHI management application would indicate when changes were made (and by whom) and some will permit an administrator to roll back unauthorized changes to a previous version. When researching the purchase of such an application, Covered Entities should look for these features in candidates and may consult with the UNCG HIPAA Security Officer for assistance.

§164.312 (d) Person or Entity Authentication

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

There are two aspects to this standard: first, authorized employees will need to access ePHI as part of their duties and second, other individuals or organizations may have an authorized need to access ePHI or the information systems containing the data. Both groups will need to be properly authenticated prior to accessing ePHI.

For employees of a Covered Entity that stores ePHI in central ITS-provided file space, each user’s unique username and password act as a means of identification sufficient to meet this requirement.

There are other sections of this document closely related to employee authentication. As mentioned in §164.312 (a)(2)(i), Unique User Identification, the University’s Acceptable Use policy prohibits the sharing of account information. As described in §164.308 (a)(5)(ii)(C) Log-in Monitoring Procedures, an entity should look for indications that an account’s integrity has been compromised.

For persons outside of the Covered Entity, such as ITS or third-party support staff, who may need to access information systems containing ePHI, the Covered Entity should establish authentication procedures under this standard. For example, a third-party support technician might be given an account for an entity’s ePHI management software for the purposes of remote patching of the software. Such access by persons outside the Covered Entity should operate under agreements defined in advance. Access to a Covered Entity’s PHI by a Business Associate employee or agent shall be subject to the terms and conditions of the Business Associate Agreement.

§164.312 (e)(1) Transmission Security

Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.
Transmission refers to any movement of data over a network. This includes accessing ePHI stored on a central ITS-provided file server, in which the data is being transmitted from the server to your workstation.

The UNCG network is configured so that data transmissions between a client computer and the on-campus destination are not accessible to other clients on the network. If the Covered entity operates within the requirements of the University’s Security of Networks and Networked Data Policy, then this integrity will be maintained. Specifically, use of hubs is not permitted. All client devices must be connected directly to an ITS-installed network port.

It is important to note that data transmissions that leave the UNCG network must be secured in some additional manner as the integrity of the off-campus network (i.e. the Internet) cannot be guaranteed. Covered Entities are strongly encouraged to prohibit any transmission of ePHI off the campus network as a default policy and then add exceptions to the policy where absolutely needed.

If off-campus transmission of data is necessary (e.g. to transmit billing information to a clearing house), care should be taken to document the means by which the transmission is secured. Some examples would be the use of a dedicated dial-up connection to a server at the recipient’s location or the creation of an encrypted VPN (virtual private network) between the Covered Entity and the recipient for transmission over the Internet.

It is not recommended that email be used as a means of transmitting ePHI. Email is typically stored on both the sender and recipient’s workstations by the email client, archived on the sender and recipient’s mail servers, transmitted in plain text over the Internet, and accessible by the recipient from any location their email server will allow.

It is not recommended that public instant messaging programs (AIM, ICQ, Windows Messenger, et al) not be used to transmit ePHI. Public instant messaging programs operate by routing communication from the local client to the host company’s servers and then back to the recipient over the Internet. This data may or may not be accessible to third parties during transmission but it is fully accessible to the company providing the service.

Transmission of ePHI using wireless technologies (e.g., 802.11 WiFi, Bluetooth, etc.) is not recommended. While means exist for securing these technologies, the nature of the medium is such that the risk in using wireless is inherently greater than in using equivalent wired technologies.

This standard has two implementation specifications: Integrity Controls, and Encryption.
§164.312 (e)(2)(i) Integrity Controls

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

For transmission of ePHI within the campus wired network, the potential for interception and modification of the transmission is extremely low. Additionally, by using the authentication methods described in §164.312 (c)(2), namely checking a file’s hash value against that stored in the hash database, the integrity of a file may be checked against the last version recorder in the database. This is also effective in verifying a file’s condition after transmission. If the recipient is provided the hash value for a file, they can confirm that the file was not altered prior to receipt.

§164.312 (e)(2)(ii) Encryption

Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. (Addressable)

In this context, encryption can refer to several encrypted transmission methods. A VPN encrypts all data between the client and the terminating point. Accessing a secure web site uses encrypted data transmission. Files may also be securely transferred by encrypting the file (as discussed in §164.312 (a)(2)(iv) Encryption and Decryption) and transmitting the encrypted file via an otherwise insecure means, e.g. FTP. This requirement will generally vary between Covered Entities and will most likely be determined by the nature of off-campus transmission of ePHI.

In order to determine a secure mechanism, Covered Entities are encouraged to consult with the UNCG HIPAA Security Officer prior to attempting an off-campus transmission.