UNC Greensboro
HIPAA SECURITY MANAGEMENT
PROCEDURES

1. Security Management Process

UNCG develops and reviews security policies, procedures, and controls that reasonably and appropriately mitigate identified risks to UNCG information systems containing PHI consistent with applicable federal, state, and University standards.

2. Assigned Security Responsibility

2.1 Management at each Covered Entity (CE) will designate a faculty/staff member as the HIPAA Compliance Officer (CO).

- The general requirements for the HIPAA Compliance Officer are:
  1. Knowledge of CE staff and functions;
  2. In collaboration with UNCG ITS or appropriate service vendor, knowledge of information systems for their CE, including computing hardware, software, and networks; and
  3. General knowledge of HIPAA Security standards.

2.2 The HIPAA CO will collaborate with the UNCG HIPAA Committee to update UNCG policies and procedures as needed to remain consistent with applicable federal, state, and University security standards, policies, and practices

2.3 The CO will work in conjunction with UNCG Information Technology Services to:

a. Coordinate security activities with appropriate UNCG Information Technology Services (ITS) personnel;
b. Coordinate the selection, implementation, and administration of significant UNCG security controls;
c. Ensure that UNCG systems utilized presently or in the future will not compromise the confidentiality, integrity, or availability of UNCG maintained EPHI.

3. Security Evaluation

3.1 Each HIPAA Compliance Officer conducts formal annual compliance evaluations of UNCG HIPAA Security Rules for their CE. Evaluations consists of:

a. Review of effectiveness;
b. Identification of gaps between Security Rules and Security policies, procedures and practices;
c. Continued identification of threats/risks to UNCG maintained information systems; and
d. Determination of whether existing controls are adequate and, if not, recommended solutions.

4. Security Risk Analysis

4.1. Each CE completes a Security Risk Analysis or Assessment using a HIPAA Committee-approved HIPAA Security Risk Analysis process

a. The Security Risk Analysis is completed at least annually, when a security risk has been identified, or whenever operational or environmental changes occur that could potentially impact the confidentiality, integrity, or availability of UNCG-maintained EPHI.
b. Changes that can initiate an assessment are:
   i. A single significant security incident or pattern of less significant security incidents
   ii. Identification of significant new threats to IT systems
   iii. Significant changes to IT infrastructure Compliance Officer

4.2. The UNCG HIPAA Committee and HIPAA Privacy and Security Officers recommend a methodology for annual security assessments, e.g. utilizing the DHHS HIPAA online Assessment Tool.

UNC Greensboro
HIPAA SECURITY MANAGEMENT
PROCEDURES

5. **Security Risk Management**

5.1 The HIPAA Compliance Officers develop strategies to manage risks that may include:

a. Risk acceptance - an understanding that a risk is of such low probability that efforts to mitigate are considered unnecessary;
b. Risk avoidance - a strategy to negate the probability of a medium or high-risk situation by utilizing a different option with less inherent risk;
c. Risk limitation - a strategy to incorporate partial risk reduction thereby reducing or limiting the overall risk; or
d. Risk transference - a strategy to shift the risk to another entity.

5.2. The HIPAA Compliance Officers are responsible for:

a. Determining the risk prioritization of any given identified threat and assigning resources, as necessary, to mitigate the threat;
b. Selecting the method used to minimize or eliminate the identified threat;
c. Recommending the most cost-effective measure to achieve the most reasonable level of security;
d. Documenting a cost-benefit analysis whenever a specific security method is not implemented due to excessive costs; and
e. Sharing responsibility jointly with the HIPAA Security Officer for implementing and monitoring selected security measures.

5.3 An acceptable risk is defined as a risk that is reviewed thoroughly by the HIPAA Committee and determined that the likelihood or probability of a significant security incident resulting from the risk is such that efforts to mitigate the risk are beyond reasonable effort.

5.4 The HIPAA Compliance Officer of each CE forwards a findings report of the Risk Analysis to the UNCG HIPAA Privacy and Security Officers, as well as the UNCG HIPAA Committee, and determines what actions, if any, need to be taken.

a. actions taken or not taken by UNCG staff relative to findings of the HIPAA Risk Analysis are to be documented. Such actions are taken to reduce identified risks to an acceptable or reasonable level.
b. Documentation of the analysis and action plans will be stored in a designated UNCG HIPAA Committee central repository.

5.5 As part of the HIPAA Security Risk Analysis process and in conjunction with appropriate ITS support services, the HIPAA Compliance Officers maintain accurate, updated inventories of all information systems hardware, software, and UNCG staff member access permissions, along with the security measures in place to protect them.

6. **Security Information System Activity Review**

6.1 HIPAA Compliance Officers implement mechanisms through UNCG information systems that automatically track at least:

a. Date and time of system activity
b. Origin (location) of activity
c. User identification
d. Description of completed activity.

6.2 The HIPAA Compliance Officer or appropriate designee conducts at least annual audits of access to information systems in at least one of the three areas below:
a. Activity audit logs
b. Information systems access reports
c. Security incident tracking reports, defined as an external attempt to access UNCG information systems, either through a desktop or server.

6.3 HIPAA Compliance Officers implement in-depth auditing mechanisms if reviews indicate a significant threat. Examples of auditable events include:
a. Unauthorized access to EPHI
b. Unauthorized use of software programs or utilities
c. Unauthorized attempts to use a privileged account, an account having power user or
i. greater permissions
d. Unauthorized system start-ups or stops
e. Multiple failed authentication attempts
f. Identified security incidents.

6.4 Results of information systems audits are considered confidential information and:
a. Only CE HIPAA Compliance Officers and ITS staff may have access to audit reports as necessary
b. HIPAA Compliance Officers archive audit reports in designated HIPAA secure storage for ten years, then destroyed by UNCG retention guidelines, for the following incidents:
i. Successful unauthorized access to EPHI
ii. Unauthorized system start-up or stop if a significant threat to EPHI
iii. Significant security incidents
iv. Any other activity deemed to have potential legal ramifications (University Counsel may be consulted).

7. Security Awareness and Training

7.1 HIPAA training is provided for all appropriate UNCG staff on or before Covered Entity billing commences and is repeated annually.
a. Appropriate staff includes all CE staff, students and faculty that come into contact with EPHI.
b. Additional University departmental staff, as identified by the HIPAA Committee, may also be required to complete the mandated training.

7.2 HIPAA Compliance Officers are responsible for implementation of the UNCG mandated HIPAA training in CE's and maintaining training and test records.
- UNCG staff members are granted final access permissions to UNCG EPHI only after having completed adequate training and orientation.

7.3 The formalized training program includes but is not limited to:
a. Overview of UNCG HIPAA policies and procedures

b. Specific examples of the responsibility each staff member has to protect UNCG maintained EPHI
c. Introduction to UNCG ITS mandated security training
d. Security best practices, including:
    i. Password management
    ii. Methods for protection against malicious software
    iii. Information about log-in, auto log-off, and system activity monitoring on UNCG information systems accessing EPHI
e. Verification of staff participation in the formal training.

7.4 The formalized training program is competency based and requires a minimum score of 80% on follow-up testing.
a. UNCG staff failing to score 80% must retake the examination until 80% is achieved.
b. Staff who fail to achieve 80% upon retest will have previously granted access suspended until being retrained and achieving the minimum 80% score.
c. Any UNCG staff member subject to sanctions due to HIPAA violations must complete the formal UNCG HIPAA Security Awareness training and achieve an acceptable competency score.
d. Third parties with a legitimate need for access to UNCG EPHI are exempt from the UNCG HIPAA training but are expected to meet all applicable federal HIPAA requirements.

7.5 HIPAA Compliance Officers are responsible for providing all appropriate UNCG staff members with on-going updates about HIPAA security issues.

8. HIPAA Access Authorization and Modification

8.1 HIPAA Compliance Officers (CO) are responsible for:
a. Review of EPHI access needed to accomplish legitimate work assignments.
b. Establishment of access levels to UNCG-maintained EPHI needed for staff members and third parties.
c. Supervision as appropriate.

8.2 All UNCG staff/faculty with access to EPHI must comply with UNCG ITS Security policies and procedures.

8.3 Access levels are based on job functions and granted for length of employment unless:
a. Staff member changes jobs necessitating an alteration of access permissions.
b. Access permissions are removed due to compliance violations.
c. Staff member receives a time-limited task assignment requiring additional access permissions.

8.4 Access to UNCG EPHI should be user, role or context based.

8.5 Documentation of access privileges should be maintained in a secure electronic format and audited at least annually for any necessary revisions.

8.6 UNCG staff members and third parties with a legitimate need for access may gain access only after proper authorizations are made.

8.7 Access authorizations for third-party vendors are delineated in a Business Associate Agreement and should be monitored.

- Access modifications are documented to identify:
    a. Date of modification,
    b. Description of modifications,
    c. Reason for modification.

8.8 CO are responsible for terminating access to EPHI of UNCG staff by the last day of employment and returning all UNCG assets to inventory.

9. Reporting Security Incidents

9.1 All UNCG staff members are required to report as soon as possible any suspected security threat to UNCG maintained information systems accessing EPHI.

- Reports may be made to the Covered Entity HIPAA Compliance Officer or to the UNCG HIPAA Privacy or Security Officers.

9.2 The CE HIPAA Compliance Officer investigates the incident and reports to the HIPAA Privacy and Security Officers and the HIPAA Committee, including:

a. Security incident analysis
b. Cause identification
c. Recommendations for damage mitigation
d. Determination of need for a complete risk analysis. Minor security incidents do not activate a security investigatory team
e. Determination of level of threat presented:
    i. Minimal- current security controls prevented damage
    ii. Medium – security controls unable to contain damage to info system and require reassessment
    iii. Severe – security controls did not detect threat and sever damage did our could have occurred. Extensive recovery and new security controls needed.

9.3. The HIPAA Compliance Officer maintains an electronic record of the incident in approved HIPAA Committee secure storage, including:

- Incident type, costs (including staff salaries) to investigate, mitigate, and recover from the incident.

10. Security Violation Sanction

10.1 UNCG staff members who violate UNCG HIPAA Security policies are referred to their immediate supervisor(s) for disciplinary action, which depending on the severity of the violation and the potential threat to the security of UNCG EPHI could include a range of sanctions from verbal warning to loss of access permissions to termination from employment or program standing.

10.2. In all cases where a UNCG staff member has either knowingly or unknowingly committed a security violation, the staff member is required to attend additional HIPAA Security Awareness and Training, in addition to any other sanction imposed, except in situations in which termination occurs.

10.3 In no case will sanctions imposed for UNCG staff members violating UNCG HIPAA Security policies conflict with University disciplinary action policies and procedures.

10.4 UNCG staff members maintain their rights to appeal any disciplinary action as described by University policy.

a. For students, an appeal process is established, consistent with University policy. Although appeal routing may vary depending on their specific natures, appeals generally begin at the student advisor/course instructor level, then move to department chair, dean, and as necessary, to other University administrative offices. All formal appeals must be presented in writing.
b. SHRA staff will follow the Grievance policy outlined by UNCG Human Resources policies.
c. EHRA Faculty and EHRA Non-Faculty will follow Provost Office guidelines.

11. Security Business Associate Agreement

11.1 All third-party vendors with a business associate arrangement with UNCG are required to agree in writing to protect the confidentiality of UNCG-maintained EPHI in accordance with HIPAA Security Rules (see UNCG Business Associate Agreement (BAA) template on UNCG Provost Office website).

11.2 Any UNCG business Associate failing to satisfactorily comply with the requirements of the BAA are notified in writing by the HIPAA Compliance Officer and the incident is reported to the UNCG Privacy and Security Officers and the HIPAA Committee.

a. The BA is given specific information about the alleged compliance failure and given 30 days to take corrective action or to appeal.
b. The HIPAA Compliance Officer monitors the BA's performance until compliance is reestablished satisfactorily at which time the BA is informed.
c. A UNCG BA failing to comply with the security stipulations of the BAA risks contract relationship termination.

11.3 Any UNCG department failing to protect UNCG-maintained EPHI will:

a. Report the alleged failure to UNCG HIPAA Security Officer,
b. Participate in mitigation efforts, and
c. If there is failure to reach satisfactory agreement, issues will be referred to respective vice-chancellors for resolution.

12. Facility Access and Security

12.1 UNCG protects EPHI by preventing unauthorized physical access to areas where EPHI is located or accessed.

12.2 Physical security includes the following measures:

a. All UNCG clients, vendors, and research participants will check in at appropriate locations within CE's.
b. UNCG employees with legitimate need to access the facility are required to display UNCG identification with photo.
c. Access to all areas containing electronic or paper PHI is controlled through a key system controlled in coordination with UNCG's physical plant to minimize unauthorized access.
    i. Doors remain locked at all times unless an authorized person is working in the area. In cases of frequent access need during the work day, doors must be locked after hours.
    ii. Health records are not left unattended in areas where unauthorized individuals could gain access.
    iii. Original records do not leave the facility except in response to a properly executed subpoena or court order.
    iv. Secondary and inactive records are protected as original health records.

12.3 HIPAA Compliance Officers perform documented annual inventories of all physical access controls used to protect workstations at CE's.

12.4 UNCG's Physical Plant is responsible to ensure perimeters of UNCG facilities housing EPHI are physically sound and in good repair to prevent unauthorized access.

12.5 HIPAA Compliance Officers maintain documentation of reports, repairs and modifications to CE's that are related to security, including date, reason and person performing repairs.

12.6 UNCG staff members are responsible to ensure that office doors and windows are locked to prevent access.
12.7 UNCG delivery and loading areas for CE's are controlled and access for non-University delivery personnel is allowed only after identity confirmation.
12.8 All UNCG staff members are responsible for addressing and/or reporting unescorted strangers within CE's to their supervisors.
12.9 In the event of an emergency or disaster, only authorized UNCG staff members or ITS personnel may administer or modify processes and controls which protect EPHI.

13. Device and Media Controls

13.1 The UNCG ITS Department is responsible for tracking and storage of UNCG networked information systems, locations/statuses of workstations and back-ups.
13.2 Storage of EPHI on the following media are prohibited:
a. Computers (desktop and laptops)
b. Portable drives or storage devices
c. Printers
d. Fax machines
e. USB flash memory.
13.3 Storage of EPHI is restricted primarily to centrally-administered server systems in secure data center locations that are not generally accessible to users and have controls in place to limit access and movement.
13.4 Destruction of systems or devices containing EPHI is tracked and logged by HIPAA Compliance Officers or UNCG ITS with:
a. Date, time, method of disposal
b. Name of person performing disposal
c. Description of disposed electronic media or workstation.
13.5 If a workstation accessing EPHI is re-used within UNCG, the previous hard drive must be completely removed with erase tools approved by UNCG ITS.
- Removed hard drives to be stored in a secure area until re-formatted for reuse .

13.6 Permanent disposal of a workstation containing EPHI is the physical destruction (smashing, drilling, shredding, etc.) of the workstation on-site by a designated UNCG ITS member or an approved industrial data destruction service (i.e. Shred It).
13.7 UNCG ITS is responsible for destroying backup tapes and for documenting destroyed workstations and electronic media.

14. Workstation Security

14.1 All UNCG workstations with access to EPHI are located in physically secure areas and:
a. Display screens are positioned to prevent unauthorized viewing.
b. Automatically set to log off after inactivity. Staff to activate workstation locking software when leaving workstations unattended.
c. Desktop computers preferred with exceptions of laptops approved by HIPAA Compliance Officers.
d. Non-UNCG staff members in physical proximity of a computer workstation with EPHI access are monitored by UNCG staff members.

14.2 UNCG staff members are prohibited from accessing EPHI via a wireless internet connection unless specific access permission is granted by the HIPAA Compliance Officer and a VPN is used to access EPHI from information systems or workstations outside of UNCG.

15. **Electronic Communications**

15.1 All electronic communications from UNCG are to patient UNCG email accounts.

15.2 Non-secure email communication of EPHI is prohibited due to the unprotected nature of the transmission.

15.3 UNCG utilizes application software capable of encryption and decryption of UNCG maintained EPHI.

- Any application software utilized by UNCG to transmit or access EPHI is assessed to determine the strength and compatibility of it its encryption/ decryption abilities before implementation through consultation with UNCG ITS.

15.4 Unencrypted electronic communication may be sent via UNCG email notifying patients of unencrypted PHI on electronic health record patient portals.

15.5 Text messages may be sent to patients only if no PHI is contained.