University of Central Arkansas
HIPAA Security Policy and Procedures

The University of Central Arkansas is a hybrid entity and has designated Healthcare Components that are subject to HIPAA. UCA's Healthcare Components and Business Associates must comply fully with the applicable HIPAA Security Rule requirements. To that end, all such members of the UCA Workforce must comply with UCA's HIPAA Privacy Policy and this HIPAA Security Policy (this "Policy"), which are meant to complement each other and be used together to ensure that UCA meets its HIPAA obligations. In the avoidance of doubt, this Policy shall be applicable solely to UCA Healthcare Components, UCA's Business Associates, and any department or unit within the University that receives PHI from the Healthcare Components or Business Associates.

No third-party rights are created by this Policy. UCA reserves the right to amend or change this Policy at any time without notice. To the extent that this Policy establishes requirements and obligations above and beyond those required by the Security Rule, this Policy shall be aspirational and shall not be legally binding upon UCA, nor give rise to a violation of the Security Rule. Thus, individuals may not bring a private cause of action based on this Policy or on UCA's obligations under the Security Rule. Terms used and not defined herein shall have the same meaning as under HIPAA and its implementing regulations.

I. DEFINITIONS

A. "Business Associate" means an entity, other than in the capacity of a member of UCA's workforce that creates, receives, maintains, or transmits PHI for on behalf of UCA's Healthcare Component or that provides services to or for UCA's Healthcare Components where the provision of services involves the disclosure of UCA's Healthcare Component's PHI.

B. HIPAA" means the Health Insurance Portability and Accountability Act of 1996, as amended and in effect.

C. "Electronic PHI" or "e-PHI" means Protected Health Information that is transmitted by electronic media or maintained in electronic media, limited to information that UCA accesses, maintains, or transmits.

D. "Protected Health Information" or "PHI" shall have the meaning set forth in the Privacy Rule, limited to information that UCA accesses, maintains, or transmits.

E. "Privacy Rule" means the Standards for Privacy of Individually Identifiable Health Information, codified at 45 CFR parts 160 and 164, Subparts A, D and E, as amended and in effect.

F. "Mobile Device" means any UCA owned or UCA issued electronic asset provided by the University to the Workforce including, but not limited to, laptops, smartphone and tablet devices that support electronic assets, regardless of whether or not they contain Mobile Media.

G. "Mobile Media" means electronic storage material on which information is or may be recorded electronically including devices in computers and any removable or transportable digital memory medium (including but not limited to, DVDs, CDs, USB drives, thumb drives, portable drives or discs, magnetic disks and digital memory cards).

H. "Personal Device" means an electronic asset used to access UCA e-PHI that is not owned or provided by UCA to the Workforce, including but not limited to a, laptop, smartphone and tablet that supports electronic assets regardless of whether or not they contain Mobile Media.

I. "Privacy Officer" shall mean the individual appointed to assume the obligations of the Privacy Officer in the UCA HIPAA Privacy Policy.

J. "Security Rule" means the Standards for Security for the Protection of Electronic Protected Health Information, codified at 45 CFR parts 160 and 164, Subpart C, as amended and in effect.

K. "Workforce" means all members of the UCA's workforce who have access to PHI in order to perform the functions of UCA's Healthcare Components. Workforce includes individuals who would be considered part of UCA's workforce under the Privacy Rule, such as volunteers, trainees, and other persons whose work performance is under the direct control of UCA, whether or not they are paid by UCA.

II. SECURITY OFFICIAL AND CONTACT PERSON

UCA designates the Chief Information Officer, or his or her designee, as the UCA Security Official. The Security Official serves as the person who is responsible for UCA's compliance with the Security Rule and this Policy and who assists with compliance and enforcement of this Policy. Wherever this Policy refers to the Security Official, if applicable, such reference will include any person delegated by the Security Official, whether such delegation is verbal or written.

Contact information for the Security Official shall be posted on the website for UCA.

Complaints concerning UCA's compliance with this Policy shall be referred to the Privacy Officer. Complaints received by the Privacy Officer that relate to the information technology and electronic information of the University shall be resolved in consultation with the Vice President for Information Technology. Complaints received by the Privacy Officer that relate to the physical premises of the University shall be resolved in consultation with the Vice President for University Facilities. Complaints received by the Privacy Officer that arise out of a University employee's non-compliance with this Policy shall be referred to the Vice President for Human Resources.

Contact information for the Privacy Officer shall be posted on the website for UCA.

III. WORKFORCE TRAINING

A. Policy

Workforce members will receive the necessary and appropriate training to permit them to carry out their functions for UCA in accordance with this Policy.

B. Procedures

1. Identification of Workforce. The Privacy Officer, in consultation with the Security Official and University Counsel, will identify all employees and other personnel who are members of the Workforce for training under this Policy.

2. Training. The Security Official will provide for the delivery of training sessions for all current members of the Workforce regarding the Security Rule and this Policy. All individuals who join the Workforce will be trained within a reasonable time after joining the Workforce. Training for existing Workforce members will occur as UCA deems necessary and in accordance with applicable UCA policies or practices. If this Policy is materially changed, UCA will provide training related to the changes as appropriate or necessary for the Workforce within a reasonable time after this Policy is modified.

3. Documentation. The Security Official will document the time, date, place, and content of each training session, as well as the Workforce members who attend each training session. The Security Official will maintain such documentation in HIPAA compliance files for a period of at least six (6) years and shall make it available for inspection by regulatory authorities, as appropriate.

IV. PHYSICAL AND TECHNICAL SAFEGUARDS

A. Policy

1. UCA will establish and use reasonable and appropriate administrative, technical, and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of applicable Privacy Rule requirements, in compliance with the applicable provisions of the Security Rule and applicable Business Associate Agreement(s).

2. UCA will reasonably safeguard PHI to eliminate impermissible uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

3. UCA will periodically review the safeguards and will coordinate the safeguards with internal policies and procedures.

B. Procedures

1. Physical Safeguards

   a. Secure Premises. Workforce members will safeguard all e-PHI by ensuring that access to UCA's premises and workstations is secure and that auto-screen lock technology is installed on all workstations.

   b. Access Controls. UCA will create, implement, and maintain access control and validation procedures necessary to limit individual access to areas where e-PHI is accessed or maintained. These controls will apply to individuals, including but not limited to Workforce members, maintenance personnel, vendors, and associates. These controls may include, without limitation, the following:

      (i) Proper identification of any person being granted physical access to a facility or site through a verifiable source of information, such as government or employer records or authorizing identification;

(ii) Limitation of access to those sensitive areas where PHI or e-PHI are accessed or maintained to only that access that is reasonably necessary for an individual's role or function;

(iii) Documentation of access authorizations and uses, in addition to ongoing monitoring and maintenance of such records by the Security Official or by his or her designee, as reasonable and appropriate;

(iv) Issuance of identification badges that describe a person's identity;

(v) Updates to each individual's access capabilities when the individual's role, responsibility or position changes; and

(vi) Revocation or limitation of any access authorization in a timely manner when access is no longer needed.

c. UCA will develop and implement procedures to ensure that all physical safeguards are reviewed, tested, and revised on a regular basis.

2. Technical Safeguards

a. As applicable, technical safeguards will be implemented, such as reasonable and appropriate firewalls, security software, and encryption programs as well as a requirement for unique usernames and passwords for access to UCA computer files and Mobile Devices that contain PHI. Members of the Workforce will have such unique usernames and passwords.

b. All e-PHI maintained in an UCA e-mail, on a UCA hard drive, or on a Mobile Device will be authorized and will necessitate the Workforce to coordinate the activation of UCA's encryption technology to ensure that the e-PHI is secure. Workforce are prohibited from accessing Mobile Media containing e-PHI using a Personal Device.

c. When PHI is removed from electronic media, UCA Workforce will delete all e-PHI in a commercially reasonable manner to ensure that the information is permanently unreadable prior to disposal. When a Mobile Device is returned by the Workforce to the University, the Division of Information Technology shall delete all Mobile Media, including but not limited to e-PHI, before the Mobile Device is reassigned, returned to the lessor, or disposed.

V. SECURITY OF ELECTRONIC PHI

A. Policy

UCA requires reasonable and appropriate safeguards to protect the confidentiality, integrity, and availability of e-PHI; to protect against any reasonably anticipated threats or hazards to the security or integrity of the e-PHI; to protect against any reasonably anticipated uses or disclosures that are not permitted by the Security Rule; and to support Workforce compliance with this Policy and with the Security Rule.

UCA will review and modify its security measures as needed and will update documentation of such security measures periodically and as needed.

B. Procedures

1. Security Management Process

UCA maintains a security management process to prevent, detect, contain, and correct security violations of applications and/or systems that contain e-PHI.

a. Risk Analysis: UCA will conduct an assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of e-PHI held by UCA, annually or upon a significant change in the system. Such review will include the assessment of the reasonableness of encryption or other enciphering tools.

b. Risk Management: On the basis of its risk analysis, UCA will manage risks to its e-PHI by limiting vulnerabilities to a reasonable and appropriate level by taking into account various factors such as the complexity of the vulnerability; UCA's technical infrastructure, hardware, software, and security capabilities; the costs of security measures; and the criticality of the e-PHI potentially affected.

2. Information System Activity Review

The Security Official or another appropriate administrator will regularly monitor access to information systems to ensure compliance with this Policy. Access audit trails will be maintained and reviewed at least annually or in response to suspicious activity to determine whether unsuccessful logons and access attempts are occurring. The Security Official will also periodically run reports of user identification names, send a report to the administrator of the Healthcare Component(s), and update user access after a response.

3. Workforce Security

UCA maintains workforce security procedures to ensure that all members of the Workforce have only appropriate access to e-PHI.

a. Authorization and/or Supervision: Unless otherwise permitted by UCA pursuant to a Business Associate Agreement or other written agreement, only appropriate members of the Workforce will be granted access to e-PHI.

b. Workforce Clearance Procedures: The Privacy Officer or the Security Official will periodically review which members of the Workforce have access to e-PHI to determine whether the access is appropriate. UCA or the Security Official will periodically monitor access logs and audit trails to ensure that the access and use of e-PHI by each member of the Workforce is consistent with this Policy and the Security Rule.

c. Termination Procedures: If a person employed by or under contract with UCA who has access to e-PHI is terminated or resigns, the Workforce member's computer accounts will be disabled, and he or she will return all UCA assets in his or her possession or control, including access codes, control devices and Mobile Devices.

4. Information Access Management

To ensure that appropriate access to e-PHI is consistent with the Security Rule, only authorized users will be permitted to access devices or platforms containing e-PHI that is owned or maintained by UCA. UCA actively manages the rights of the Workforce to access e-PHI. To the extent that it is reasonable and appropriate, access to e-PHI is limited to members of the Workforce for purposes of carrying out their services for UCA as permitted by the Security Rule and consistent with UCA internal procedures. When a member of the Workforce is permitted access to e-PHI, UCA will define the scope of such access based on each Workforce member's need to access such e-PHI to perform his or her job functions. UCA will terminate or modify the scope of a member's access as appropriate or necessary due to modified employment position or other applicable rationale.

Access to devices or platforms containing e-PHI that is owned or maintained by UCA will be restricted through the use of username and password verification according to standards set forth by the University's Division for Information Technology's Policy on Data Classification and Handling. In addition, UCA will implement auto-screen lock on all Workforce workstations.

5. Mobile Devices and Media

a. Protecting Mobile Devices. All users of Mobile Devices and Mobile Media, whether the equipment or media is a Personal Device or is owned by UCA, assume responsibility for ensuring compliance with this Policy. This means that Workforce have an individual responsibility to take the necessary precautions described in this Policy to prevent potential theft of ePHI. When traveling, Workforce should be aware of the location and circumstances of the Mobile Device at all times and may additionally take the following measures to protect the Mobile Device: (1) on flights, carry the Mobile Device and Mobile Media in your hand luggage; (2) in a vehicle, lock the Mobile Device and Mobile Media in the luggage compartment when you leave the vehicle; (3) in hotels, lock the Mobile Device and Mobile Media in a safe or cabinet; and (4) in public areas, never leave the Mobile Device and Mobile Media unattended.

i. No ePHI shall be maintained on Mobile Devices or Mobile Media unless authorized and necessary and Workforce has caused UCA's encryption program/system functions to have been activated to ensure that the ePHI is secure.

b. Unauthorized Access; Password Protection. A Mobile Device and Mobile Media must be protected against unauthorized access at all times. Workforce must take reasonable actions to secure the Mobile Device. Password protection must be enabled on all Mobile Devices to protect against information loss should the Mobile Device be lost or stolen.

c. Stolen or Lost Mobile Device or Media. If any Mobile Device or Mobile Media is lost or stolen, the Workforce must report this immediately to the Privacy Officer and Security Official and advise if any confidential information was contained on the Mobile Device or Mobile Media. Personal passwords must be immediately changed. UCA may remotely wipe or otherwise disengage any data or program on the stolen or lost Mobile Device or Mobile Media to limit risks to confidentiality of material maintained on the mobile device.

d. Removal from UCA Facilities. Workforce may take Mobile Devices and Mobile Media out of UCA's facilities only within the framework of the duties assigned to them and the work required of them. The Workforce assumes personal responsibility for taking any protective measures that may be necessary during transport, use, and storage, including but not limited to encryption where reasonable and appropriate, and for returning UCA's equipment and information intact.

e. Personal Devices. Workforce are prohibited from accessing ePHI using a Personal Device.

6. Reuse or Disposal of Electronic Media

In the event UCA determines e-PHI maintained by UCA should be destroyed, UCA will permanently erase or destroy e-PHI in accordance with HIPAA and any applicable provisions of state law. In the event UCA determines that certain electronic media containing e-PHI must be disposed of or reused for another purpose, UCA will ensure all e-PHI maintained on such device is permanently erased or wiped of all e-PHI. The maintenance of e-PHI will be in accordance with the standards of this Policy and as required by the Security Rule until such time as it is erased or destroyed.

7. Contingency Plan

UCA maintains a contingency plan that includes procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, or natural disaster) that damages systems and/or applications containing e-PHI. To the extent necessary and required by the Security Rule, UCA will create and implement the following components of a contingency plan:

a. Data Backup Plan: UCA will maintain data backup systems that allow for the maintenance of retrievable exact copies of e-PHI. Such data backup systems will include all security measures reasonable and appropriate for secured storage of e-PHI as required by the Security Rule and this Policy.

b. Disaster Recovery Plan: UCA will identify and implement appropriate preventive controls, such as generators, fire suppression systems and detectors, data colocation, and scheduled back-ups for hard drives and media that will be employed in the event of a disaster for purposes of restoring lost data.

c. Emergency Mode Operation Plan: UCA administrators from the IT Departments will design and implement strategies to prioritize system restoration, mitigate loss, and identify chains of command and response.

In addition, regular planned testing and response training will be performed to ensure readiness.

8. Evaluation

UCA will perform periodic technical and nontechnical evaluations based on the standards set forth in the Security Rule, to ensure that UCA's policies and procedures are updated as warranted by changes in UCA's environmental or operational conditions affecting the security of e-PHI. Such evaluation will be achieved through the collective efforts of UCA's Security Official, Vice President for Facilities and University Counsel.

VI. SANCTIONS FOR VIOLATIONS OF SECURITY POLICY

A. Policy

Employees who violate this Policy may be subject to disciplinary measures, consistent with any applicable collective bargaining agreement, up to and including suspension, dismissal, and termination.

B. Procedures

During training, the Workforce will be informed that disciplinary actions may be imposed if this Policy is violated. Appropriate disciplinary actions will be determined on the basis of the nature of the violation, its severity, and whether it was intentional or unintentional. Such disciplinary actions may include, without limitation, verbal warnings, written warnings, probationary periods, and termination of employment. Application of any disciplinary actions will be documented in accordance with UCA's record retention procedures.

The Vice President for Human Resources will determine whether, and to what extent, disciplinary action should be imposed for a violation of this Policy.

VII. UNAUTHORIZED DISCLOSURES OF PHI

A. Policy

To the extent possible, UCA will mitigate any harmful effects that become known to it of a use or disclosure of an individual's PHI in violation of this Policy.

The Security Official and Privacy Officer, in consultation with University Counsel, will coordinate the reporting of any use or disclosure of PHI that is not permitted or required in accordance with HIPAA, the Security Rule, and any applicable underlying contractual agreement. This includes reporting Breaches and Security Incidents of which it becomes aware, in accordance with HIPAA reporting requirements and the UCA HIPAA Privacy Policy.

B. Procedures

If a member of the Workforce becomes aware of a disclosure of PHI, either by a member of the Workforce or by an outside consultant or contractor, that is not in compliance with this Policy, the Workforce member will report the disclosure to the Privacy Officer. This may be accomplished through the Workforce member's supervisor.

The Privacy Officer shall consult with the Security Official and University Counsel to determine if the incident rises to the level of a Breach requiring notification.

The Privacy Officer will document such incidents, and as necessary in consultation with the Security Official, will investigate, mitigate, and track the effects of such incidents.

VIII. DISCLOSURES OF PHI TO BUSINESS ASSOCIATES

A. Policy

Members of the Workforce may disclose PHI to UCA's Business Associates in accordance with the UCA HIPAA Privacy Policy and terms of any applicable underlying Business Associate Agreement. UCA may act as a business associate if any unit or department within UCA creates, maintains, uses, or transmits PHI on behalf of the Healthcare Components.

B. Procedures

1. Disclosure to Business Associates: All uses and disclosures of PHI by or to a Business Associate must be made in accordance with a valid written Business Associate agreement that complies with the requirements of the Privacy and Security Rules. All disclosures to a Business Associate must comply with the "Minimum Necessary" standard. If a member of the Workforce becomes aware of a pattern or practice that may be a material violation of the Business Associate's duties with respect to this Policy or the Privacy Rule or Security Rule, the member of the Workforce will notify the Security Official and Privacy Officer directly or through the member's supervisor.

2. UCA as a Business Associate: If any department, division, unit, school or college of UCA receives, maintains, uses or transmits PHI on behalf of an UCA Healthcare Component, such department, division, unit, school or college of UCA will adhere to the UCA HIPAA Privacy Policy, the UCA HIPAA Security Policy, and the Privacy and Security Rules.

    a. When UCA contracts for services and subcontractors have access to PHI, UCA will require each Subcontractor to agree, in writing, that it will reasonably safeguard PHI in accordance with the Business Associate Agreement(s) in the HIPAA Privacy Policy.

IX. STATE LAW PREEMPTION

A. Policy

In the event that applicable state laws are more stringent then HIPAA, UCA will comply with those laws.

X. RECORD RETENTION AND DISPOSAL

A. Policy

UCA will maintain documentation supporting compliance with this Policy, including audit logs, risk analyses, training completions, and Workforce sanctions, in accordance with internal and state record-retention requirements.

UCA will dispose of records, including PHI, in accordance with its HIPAA Privacy Policy.

XI. Related Policies.

- UCA Board Policy 412, Computer Use
- UCA HIPAA Privacy Policy
- UCA Mobile Device Security Policy
- UCA Network Security Policy
- UCA Network Password Policy
- UCA User Account Management Policy
- UCA Remote Access Policy
- UCA Safeguarding System Passwords Policy

INDEX

Page