

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

**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  
[redacted] would be considered part of UCA's workforce under the Privacy Rule.

[REDACTED]

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

[REDACTED]

members will receive LICA deemed necessary and in accordance with applicable

[REDACTED]

- (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

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

a. As applicable, technical safeguards will be



a. Authorization and Access: 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.



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.

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 Mob 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

c

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.

[REDACTED]

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 evaluations will be achieved through the collective efforts of UCA's Security Official, Vice President for

[REDACTED]

Facilities and University Counsel.

VI. SANCTIONS FOR VIOLATIONS OF SECURITY POLICY

A. Policy



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**

[REDACTED]

the UCA HIPAA Privacy Policy and terms of any applicable underlying Business Associate Agreement.

UCA must not be a business associate if any unit or department within UCA creates, maintains, uses, or

[REDACTED]

**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.



