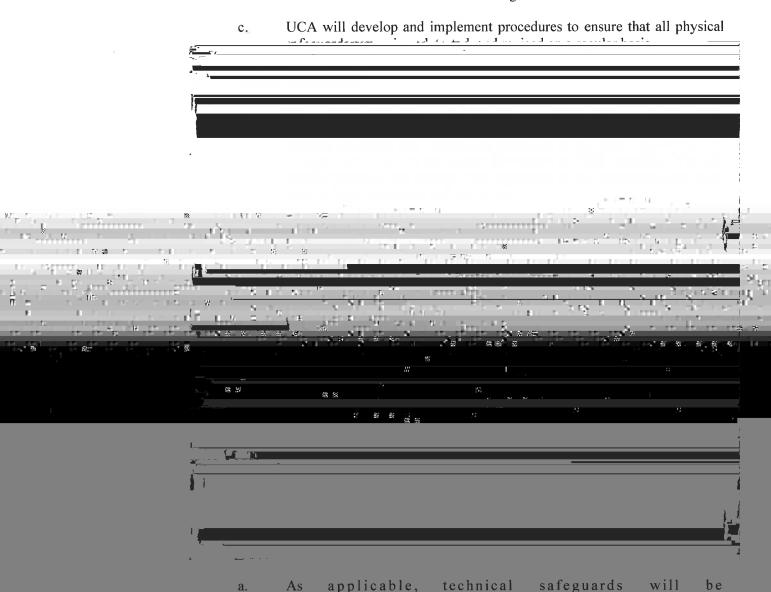


that are subject to HIPAA. UCA's Healthcare Components and Business Associates must comply fully with the applicable HIPAA Security Rule requirements. To that end, all such members of the UCA

	A	"Personal Device" means an electronic asset used to access UCA e-PHI that is not owned
. · -		
	•2	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.
	17.	MILL OF COURSE OF The LICAR World forms who have access to DUI in
7		
. —		
		<u> </u>
,		
4		
*		
		order to perform the functions of UCA's Healthcare Components. Workforce includes

	: !
\· \·	
l _i —	
1	
ŧ	
	-
	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
	INK B
ı	n contract mill account a LICA decree account and in account and with contracts
	i I
	i de la companya de
à	

- (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.



V. SECURITY OF ELECTRONIC PHI

A. Policy

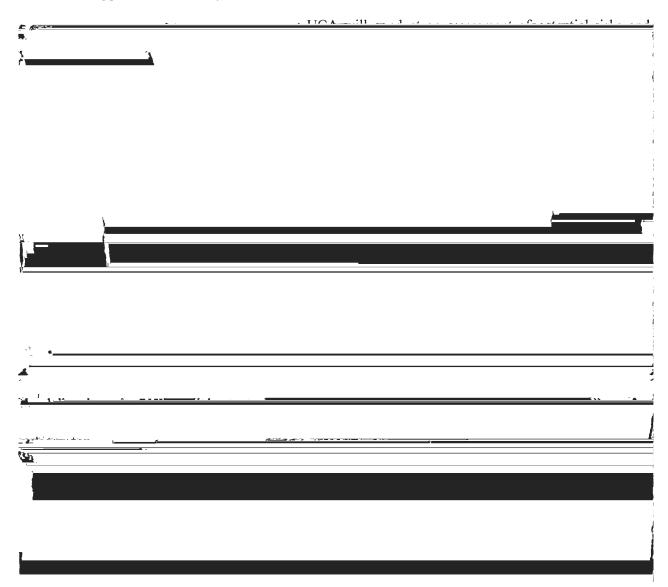
UCA requires reasonable and appropriate safeguards to protect the confidentiality, integrity, and availability of e-PHI; to protect against any reasonably anticipated threats or hazards to the security or integrity of the e-PHI; to protect against any reasonably anticipated uses or disclosures that are 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.

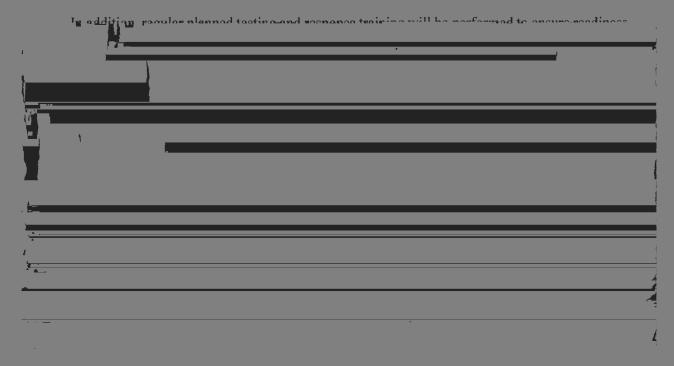


	a	Authorization and Unless otherwise permitted by UCA pursuant to a Business Associate Agreement or other written agreement only appropriate members of the Workforce will be granted access to e-PHI.
}	b.	Workforce Clearance Procedures: The Privacy Officer or the Security Official will periodically review 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 World process of the Security Pulls
<u> Anna anna anna anna anna anna anna ann</u>	_	
7		
,	_	
	_	
	_	
	_	
-		
5		

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

				A Mobile Device
and Mobile Media mur reasonable actions to se				
Devices to protect again				
	c. Stolen or I	Lost Mob	If any Mo	obile Device or Mobile
Media is lost or stolen.	the Workforce mus	st renort this imme	diately to the Privac	v Officer and Security
		_		
				â
Official and advise if an				
Personal passwords mus	t be immediately c		remotely wipe or ot	herwise disengage any
A CONTRACTOR OF THE PARTY OF TH				
·				
₽ =				
-				
V _G				
				ĺ
,				!
				t de la companya de
		1		
7-				
,				

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



8. Evaluation

C

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



Facilities and University Counsel.

VI. SANCTIONS FOR VIOLATIONS OF SECURITY POLICY

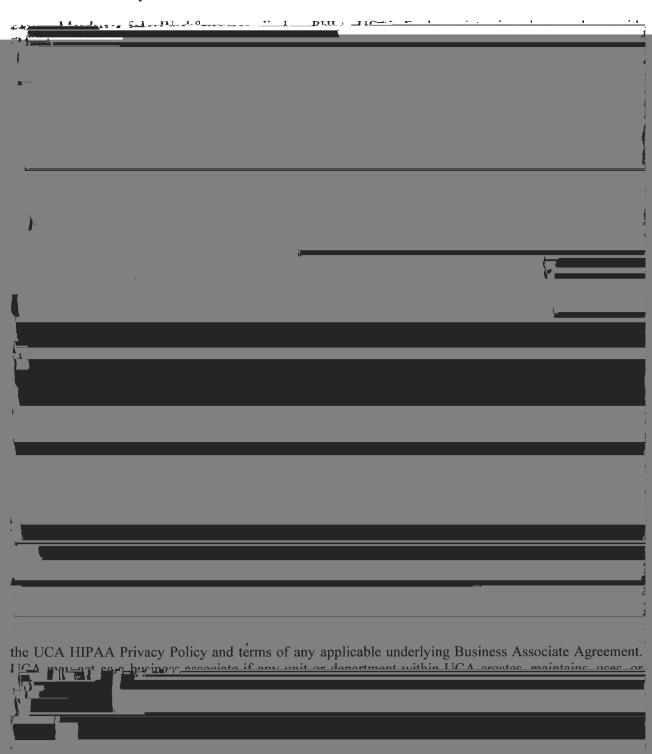
A. Policy

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



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.



INDEX

		Page
I.	DEFINITIONS	1
II.	SECURITY OFFICIAL AND CONTACT PERSON	2
III.	WORKFORCE TRAINING	2
IV.	PHYSICAL AND TECHNICAL SAFEGUARDS	3
V	FECUDITY OF ELECTRONIC BUIL	5
·	<u> </u>	
	RELATED POLICIES	<u> </u>
VI.	SANCTIONS FOR VIOLATIONS OF SECURITY POLICY	8
VII.	UNAUTHORIZED DISCLOSURES OF PHI	8
VIII	DISCLOSURES OF PHI TO BUSINESS ASSOCIATES	9
IX.	STATE LAW PREEMPTION	9
X.	RECORD RETENTION AND DISPOSAL	10
XI.		11