I. **PURPOSE**

The purpose of this document is to provide the policy and procedures to be followed by UC Irvine Healthcare in evaluating, remediating and managing potential risks to the confidentiality, integrity and availability of electronic protected health information. This policy lays the framework for a formal risk management program by establishing responsibility for risk identification and analysis, security planning for risk mitigation, and program management and oversight. Program management and oversight is a university-wide responsibility that includes the active involvement of executive leadership, departmental management, data stewards, and others with information management responsibility.

II. **GOAL**

- Confidentiality of information will be assured
- Integrity of information will be maintained
- Availability of information to authorized users will be met.
- Regulatory and legislative requirements will be fulfilled
- Information security training will be available to all staff
- Breaches of information security, actual or suspected, will be reported to, and investigated by the Information Privacy & Security functions of UC Irvine Healthcare

III. **BACKGROUND**

The federal Health Insurance Portability and Accountability Act Standard, the “Security Rule”, requires a health care covered entity to conduct an assessment of the risks to the security of electronic protected health information on a regular basis, and develop a risk management plan to reduce the identified risks to the patient information. This policy outlines the process by which UC Irvine Healthcare conducts that assessment and mitigates identified risks to the extent possible.
IV. **SCOPE**

This policy applies to all digital and otherwise electronically stored information whether it is located in computer files, equipment, or other hard assets where information is stored. It encompasses the many locations in which protected health information resides including the medical center campus, main campus and all other areas where the UC Irvine Healthcare enterprise conducts business.

V. **DEFINITIONS**

*“Addressable”* A variance on the implementation of the HIPAA security rule is allowed. If the implementation specification is not reasonable and appropriate (1) Document why it would not be reasonable and appropriate to implement specification; and (2) implement an equivalent alternative measure as determined by the covered entity.

*“Data Steward for PHI”* is any UC Irvine Healthcare workforce member who receives and reviews requests for PHI, provides access to or released PHI as permitted or required by HIPAA, prevents access to or disclosure of PHI as permitted or required by HIPAA, or serves as UC Irvine Douglas Medical Center’s liaison to the patient when the patient wants to exercise their Patient Rights provided by HIPAA or state law.

*“Electronic Protected Health Information” or “ePHI”* is any electronic information that is created or received by a health care provider that relates to the past, present, or future physical or mental health of an individual, and identifies the individual. This includes ePHI that is created, received, maintained or transmitted. For example, ePHI may be transmitted over the Internet, or stored on a computer, a CD, a disk, magnetic tape or other media.

*“Functional Area Contact”* is the individual designated by the Security Officer to coordinate the completion of applicable Information Security Assessments, and oversee the ongoing Security Management Plan for their assigned functional groups.

*“Risk”* is the potential of harm to the University or its stakeholders.

*“Risk Assessment”* Is a qualitative or quantitative evaluation of the nature and magnitude of risk to University information. The evaluation is based upon known or theoretical vulnerabilities and threats, as well as the likelihood of the threats being realized and the potential impact to the University and its stakeholders.

*“Risk Management”* Is the process of evaluating and responding to risks to University information for the purpose of reducing those risks to acceptable levels. Risk management is inclusive of the risk assessment process, and uses the results of risk
assessments to make decisions on the acceptance of risks or on taking action to reduce those risks.

“Required” Implementation specification of the HIPAA security rule is not optional.

“Restricted information” describes any confidential or personal information that is protected by law or policy and that requires the highest level of access control and security protection, whether in storage or in transit.

“System Owner” is the individual or department designee primarily responsible for the content and functioning of an electronic computer resource.

“System Administrator” is person responsible for the daily operation and maintenance of an electronic computer resource.

“Information Security incident” is a violation or imminent threat of violation of computer security policies, Information Security safeguards, acceptable use policies, or standard security practices that impacts the confidentiality, integrity and availability of health information.

“Workstation” means an electronic computing device, for example, a lap or desk computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

VI. POLICY

A. Information Security Management Governance

1) Senior Management

CEO, CIO, Dean of the School of Medicine

Roles and responsibilities:

a. Ensure an enterprise information security program is established and sustained with appropriate and adequate resources.

b. Provide direction and support for the enterprise information security Goals and Objectives.

c. Set the organization’s cultural and managerial tone for risk management and security through top-level policies

d. Designating appropriate personnel to oversee the information security program
2) HIPAA Privacy & Security Committee

The committee is composed of representatives or designees from the following areas or individuals as listed:

Director, Human Research Protections
Operations Manager, Human Resources
Information Security Officer
Assistant Dean, Academic Administration
Chief Medical Information Officer
Director, Nursing Education
Director, Risk Management
Director, Health Information Management
Chief Operating Officer
Sr. Dir., Ancillary Services
Assistant Director, Ambulatory Care
Compliance & Privacy Official
Health Science Manager, Internal Audit
Privacy Analyst
CAO – Dept. of Medicine
Chief Ambulatory Care Officer
Research Compliance Officer
Chief Administrator, Clinical Services

Roles and responsibilities:

a. Provide interdisciplinary input and guidance for the development and maintenance of information security management policies, procedures, standards and guidelines;

b. Provide oversight and guidance to assure that the information security management plan is in compliance with applicable federal, state and local laws / regulations and University policy;

c. Provide cross departmental input and support to ensure HAIS workforce members receive appropriate information security awareness training;

d. Examine potential and/or actual areas of non-conformance and recommend, develop and ensure corrective action or sanctions designed to address areas of actual or potential noncompliance.

3) Information Security Officer (ISO)

Roles and responsibilities:
Direct and update the HIPAA Security Compliance Program to assure compliance with current HIPAA Security regulations. Oversees Security Risk assessment of the UC Irvine medical enterprise clinical information systems, and implements an effective Risk Management Plan to minimize risks to the confidentiality, integrity and availability of electronic Protected Health Information (PHI). Coordinates audits of UC Irvine information systems to ensure compliance with information security requirements and policies. Provides education and training to UC Irvine Healthcare workforce members on HIPAA security policies and procedures. Develops and assists in the implementation and maintenance of UC Irvine information security policies and procedures in coordination with the Chief Compliance and Privacy Officer, the Chief Information Officer, and Legal counsel.

4) Information Security Team (IST)

Information Security Officer
HAIS Director of Technology
HAIS Security Team Lead

Roles and responsibilities:

a. Providing technical vision and leadership in support of the continued development of UC Irvine HAIS security architecture;
b. To develop and maintain information security management policies, procedures, standards and guidelines;
c. Collaborate in developing the annual information security review and workplan;
d. Directing all HAIS network security tasks and assessments;
e. To provide HAIS information security management oversight assuring compliance with the HIPAA Security Rule;
f. To develop and implement procedures for detecting, reporting, and responding to security incidents;
g. To oversee a risk assessment process and provide assessment reports;
h. Ensuring that workforce members receive appropriate information security awareness training.
B. Information Security Safeguard Standards

The UC Irvine Health Care Information Security Management program includes the following specific safeguard standards to ensure the confidentiality, integrity, and availability of all electronic protected health information:

- Administrative safeguards
- Physical safeguards
- Technical safeguards

1) Administrative safeguards

a. Standard: Security management process - The following safeguards are administered to reasonably prevent, detect, contain, and correct security violations.

1. Information Security Risk Analysis (Required)

   i. External Risk Analysis / Assessment:

   UC Irvine Health Care participates in a risk assessment of its Information Technology General Controls (ITGC) performed by an external audit vendor such as Price Waterhouse Coopers (PWC).

   ii. Information system security assessments:

   UC Irvine Healthcare shall conduct an Information Security Assessment to identify the electronic information resources that require protection, and to understand and document risks from potential threats and vulnerabilities to electronic resources that may cause loss of confidentiality, integrity, or availability of ePHI or adverse impact to an individual’s privacy. Such risk assessments will take into account the potential adverse impact on the University’s operations, assets and reputation. The Information Security Assessment will be utilized to develop and maintain an ongoing Security Risk Management Plan to identify and reduce ongoing and potential new risks.

iii. Periodic risk evaluation of Irvine Health Care core computing infrastructure and security administration.

   This periodic assessment serves to evaluate the overall IT infrastructure organization, including network flow architecture, system integration and security program administration. From this a security work plan is developed and proposed to hospital administration for approval and implementation support.
iv. The risk assessments and or report summaries will be available to the UC Irvine Privacy and Security Governing Board.

v. The UC Irvine Security office will inform UC HIPAA Privacy and Security Official(s) within thirty (30) days upon completion of documented risk assessments, and provide a copy upon request.

2. Risk Management (Required)

Security measures and controls sufficient to reduce risks and vulnerabilities as identified in the risk assessment will be implemented to reasonable and appropriate levels.

3. Information System Activity Review (Required).

Regular review of information system activity, such as audit logs, access reports, and security incident tracking reports will be performed. Documenting the incidents, implementing remediation strategies, reporting to management, and complying with legally mandated notification requirements will be performed by the Compliance Office.

4. Sanctions (Required).

Sanctions will be taken against Workforce members who fail to comply with UC Irvine Healthcare’s privacy and security policies and procedures.


b. Standard: Assigned Security Responsibility -

The Information Security Officer shall coordinate the implementation of the safeguards required under this policy, including the development and implementation of information security policies and procedures. (see also of this policy, Section VI. A. Information Security Management Governance).


Policies and procedures are implemented to ensure that all members of the workforce have appropriate access to electronic protected health information, as described under the Information Access Management standard below (see Administrative Safeguards, section 1. D) and to prevent those workforce members who are not authorized access from obtaining access to electronic protected health information.
1. **User Authorization and/or Supervision (Addressable)**

   Through the University hiring process, workforce members are assigned supervisors / managers and are deemed authorized to work with electronic protected health information as needed to perform their assigned job duties. System access authorization is described below in The Information Access Management section.

2. **Workforce Clearance (Addressable)**

   All medical center workforce members offered employment are required to pass a drug screen and successfully complete a background check prior to starting work. Individual system data stewards determine and provide access of a workforce member to electronic protected health information as appropriate to the scope of the member’s assigned duties and responsibilities.

   (See UC Irvine Healthcare General Administrative Policy “Background Check” for details).

3. **Termination Procedures (Addressable)**

   An automated separation / termination process managed by UCI Human Resources is used by medical center department managers when a workforce member employment ends. This process includes automatic notification to data stewards that trigger the deactivation of information system access. UCI Network account access is also deactivated through this process.

d. **Standard: Information Access Management**

1. **Access Authorization, Establishment and Modification (Addressable)**

   Access to computers containing PHI is controlled by confidential access codes (sign-on) and unique passwords. Authority to determine access levels for staff and faculty is the responsibility of the appropriate Director, Department Head or Data Steward and is granted according to need in order to conduct medical center business and perform job functions.

   User access code requests must be submitted in writing using the Information Services Computer Access Application Form. The form is completed by the appropriate supervisor, coordinator, department head or director. Authority to request codes can be delegated to identified user/training coordinators.
System data stewards modify the user’s right of access to electronic protected health information as appropriate to the scope of the member’s assigned duties and responsibilities.

(See UC Irvine Healthcare General Administrative Policy “Computer Access Codes” for details).

e. Standard: Security Awareness and Training

1. Formal Security Training (Required)
   The University has implemented a plan of information security education throughout the institution that will promote an on-going understanding about information security risks and recommended practices.

   UC, Irvine Health Care has a multi-pronged approach to training and awareness. Current strategies include:

   a. An overview of information security awareness is part of all new hire orientation training. Continuing education on information security is included as part of the required annual training program for each workforce member.

   b. An information security website that serves as a common repository of information security educational materials, current issues, policies and practices

2. Security Reminders (Addressable)
   Periodic communiqués are provided to the University community alerting UC, Irvine Health Care personnel to specific vulnerabilities. These Come in the form of emails via “Compliance Tips of the Week” or on an as needed basis.

3. Malicious Software protection (Addressable)
   All computers that connect to the UCI Medical Center campus IT infrastructure, including all off-campus computers that connect remotely (e.g., via wireless, VPN, or dial up) should be protected with anti-virus/malware software. All antivirus/malware software shall conform to UCI Medical Center HAIS software standards and shall have up-to-date virus definitions. This policy applies to all desktop and laptop computers, regardless of ownership or location.

   Anti Virus/Malware software will be installed such that all settings are password protected and may not be altered in any manner that reduces the effectiveness of the software.
Each deployment of Anti Virus/Malware software shall be configured to ensure automatic regular updates of virus definitions.

4. Access Monitoring (Addressable)

Log files of system activity identifying individuals who have accessed PHI are available from each information system. Evaluation of log files is performed to determine if inappropriate access to PHI has occurred. Inappropriate access would include any access not necessary in the course of the workforce performing their job duties at UCIHS.

Automation of system access monitoring is accomplished using a third party software tool that provides daily reports of system access. These reports are reviewed and acted upon by the Compliance Office.

In addition to the automated access monitoring tool, random access monitoring is performed manually as directed by the system data stewards or Compliance Office. An on-line incident report is completed in the event inappropriate access is suspected by the Data Steward.

5. Password Management (Addressable)

Electronic systems containing restricted information must be password protected to control access to restricted information. Password protected access serves to maintain the confidentiality and integrity of electronic data as well as to help protect the University's computing resources and infrastructure. The HAIS PASSWORD policy for accessing the HealthCare network establishes a minimum standard for creation of strong passwords, the protection of those passwords, and the frequency of password change.

HSNetID passwords expire every 435 days and must:

i. Have at least 8 characters
ii. Not be longer than 32 characters
iii. Have upper and lower case characters
iv. Have at least one letter and one number
v. Not be constructed from or be a match to a dictionary word
vi. Not be a profile or user name
vii. Not be a reversed profile or user name
viii. Not be a scrambled profile or user name
ix. Not be a password used within the last 730 days
x. Not have more than one pair of repeating characters
xi. Contain characters that are typed on a standard English keyboard
xii. Not contain consecutive characters on a keyboard (ie abcd, asdfg)
(See 1. UC Irvine Healthcare General Administrative Policy “Computer Access Codes” 2. HAIS HSNetId Password Complexity standard).


1. Information Security Incident definition

An Information Security incident is a violation or imminent threat of violation of computer security policies, Information Security safeguards, acceptable use policies, or standard security practices that impacts the confidentiality, integrity and availability of health information.

Examples of information privacy and security incidents include but are not limited to the following:

1. Distribution of an email or fax to the wrong recipient
2. Unauthorized access to electronic patient information
3. Unauthorized disclosure of patient information
4. Electronic media such as a laptop, CD, PDA, computer hard drive, or other similar equipment is stolen or missing and contains unencrypted personally identifiable information.
5. Unauthorized access to University servers or devices by external sources (hacking).
6. Computer security intrusion
7. Unauthorized use of systems or data
8. Unauthorized change to computer or software
9. Loss or theft of equipment used to store private or potentially sensitive information
10. Denial of service attack
11. Interference with the intended use of information technology resource
12. Compromised user account

a. Information Security incident Reporting responsibilities and methods

If a UC Irvine Healthcare Workforce member (employee) discovers that there has been an Information Security incident or suspects that an incident or breach has occurred they must immediately report the Incident Reporting Method:

Entry into the online Incident reporting system (https://intranet.ha.uci.edu/incidentreport/)
The breach should also immediately be reported directly to

Privacy Officer 1-714-456-3674

Information Security Officer 1-714-456-7349

If these officers cannot be immediately reached, the breach should be reported on the Compliance Office Alert Line at extension 7006 at toll free at 1-888-456-7006

(See UC Irvine Healthcare General Administrative Policy “Incident Reporting, Automated” for details).

See also UCOP Privacy and Data Security Incident Response Plan policy.

b. Post-Incident review and corrective action

The Incident report will be reviewed as needed by the Compliance and Privacy Officer, Legal Counsel, and Risk Management.

Interference with the intended use of information technology resource such as computer security intrusion will be referred to and addressed immediately by Technical staff from HAIS to implement corrective action to stop the event or prevent recurrence of the incident.

The Compliance Office will make a determination as which if any of the notification requirements have been triggered under both State and Federal law. The applicable notices will be made to the effected individuals and to the applicable State and federal authorities, and through media outlets as required under Federal law.

Use of the information gathered through the Incident Report process is reviewed, trended and utilized to develop corrective or process improvement plans. Those plans are then implemented, as appropriate and evaluated on an ongoing basis.

g. Standard: Contingency Plan. - The University has made provision for responding to an emergency or other occurrences (for example, fire, vandalism, system failure, and natural disaster) that damages systems containing electronic protected health information.
1. **Data backup Plan (Required).**

Backing up digital communications, data and other electronic files is an essential practice to ensure against the loss of valuable information and the ability to conduct our mission. The purpose of performing back-ups is to be able to restore a system to a known state (as of the date of the most recent back-up) in case of system failure or a catastrophic data loss event.

All PHI data hosted in the UC Irvine Medical Center Data Center, unless otherwise requested, at a minimum will include back-up (duplicate) copies of the data. These copies are stored in a protected and secure location and moved to an off-site storage location within one month of creation. The backup process uses either data copied to tapes or replicated to an alternate storage area network (SAN). In both cases, the data is transferred and housed at an off-site secure facility.

Documentation that indexes the data backups and their storage locations is maintained by HAIS. This information is also maintained and kept with the storage systems and the data themselves. This provides a means to identify and retrieve the appropriate data in the event the on-site documentation is destroyed.

For example, backup tapes that are sent to an off-site vendor (i.e. Iron Mountain) are recorded in the backup server’s media database. Hardcopy data indexes are also stored with the backup tapes themselves.

In the event of a disaster resulting in the loss of the primary data stored at UC Irvine, data recovery is accomplished by retrieval from the off-site storage.

Protocols documenting system recovery using the retrieved backup media is maintained in HAIS.

Periodic testing of Data recovery from backup media is conducted and documented by HAIS. This “testing” may also include actual recovery events.

2. **Disaster Recovery Plan (Required).** Restoration of system availability and data recovery are crucial for ensuring continuity of business and patient care operations and the safety of staff and patients.

Details of the Disaster Recovery process is provided in the UC Irvine HAIS Policy “Contingency / Disaster Recovery Plan” policy.

During an interruption of electronic information services, either by forces of nature or system failures, provision of critical patient care and business functions including the availability of a complete medical record will continue by implementing an Emergency Mode Operation Plan, also referred to as “Computer Downtime” mode.

If the interruption of electronic services is a result of an internal or external disaster, UC Irvine Hospital Incident Command System (HICS) may be instituted. This system provides for a command structure and processes to ensure continuation of operations.

When there is loss of electronic facility access control, staff will provide manual access provisioning and added space surveillance to guard against unauthorized physical access to PHI. UC Irvine Police may be enlisted to support UC Irvine staff in maintaining the security of PHI and other critical assets.


(See UC Irvine Healthcare General Administrative Policy “Computer Downtime: Backup and Recovery” for details for periodic testing and revision of contingency plans).

5. Applications and Data Criticality Analysis (Addressable).

Assessment of the relative criticality of applications and data is obtained and documented by HAIS. Criticality levels include Mission Critical, Patient Care and Standard designation. This designation is recorded in the HAIS application inventory database.

h. Standard: Evaluation (Required).

A periodic technical and nontechnical evaluation is performed, 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 HIPAA subpart (164.308(a)(8)).
See Administrative safeguards section of this policy 1. Information Security Risk Analysis item iii. Periodic risk evaluation of Irvine Health Care core computing infrastructure and security administration.

2) Physical Safeguards

a. Standard: Facility Access Controls. The following policies are implemented 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.

1. Contingency Operations (Addressable). 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 are governed by the Hospital Incident Command System (HICS).

2. Facility Security Plan (Addressable). Facilities and the equipment therein are safeguarded from unauthorized physical access, tampering, and theft. Centralized computer facilities that house core data is protected in a secure location with physical access controlled by HAIS. Computer facilities that process departmental data may require physical security depending on the value and sensitivity of the data they process, the resources they access, and their cost. Examples of facility physical safeguard security would include locating data storage behind locked doors, limiting access to a building via a controlled reception desk, video surveillance of building access point among others. Physical security management of these departmental resources is the responsibility of the department.

3. Access Control and Validation Procedures (Addressable). The following policies are implemented 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.

UC Irvine workforce members must carry and display UC Irvine identification badge in accordance with procedures established by UC Irvine Human Resources. Building access is controlled and restricted by the use of keyless electronic locks activated by the badges.

Visitor and vendor physical access is controlled at hospital entrance points with the use of staffed reception areas. All visitors must sign in to a visitor log and receive a visitor badge. The visitor badge identifies that this person is restricted from all areas where they could gain access to protected
information. All staff is trained to be on guard to insure that visitors are permitted only in non-restricted areas. Vendors requiring access to software or hardware for maintenance or troubleshooting will be escorted and overseen by UC Irvine workforce members.

Vendor Access is managed with the RepTrax system. Vendors visiting the medical center or ambulatory areas must register through RepTrax, schedule an appointment to meet with a specified individual. When the vendor arrives a badge with a photo Id is printed from the RepTrax Kiosk that identifies the vendor and who they are here visiting.

(See UC Irvine Healthcare General Administrative Policy “Visitor Access” for details).


   i. UC Irvine Medical Center Facilities requires all repairs and modifications to the physical components of the facility to be recorded in the Request for Service (RFS) on-line system. This documentation is maintained for 7 years by facilities management.

   ii. Altiris IT asset management system is used to track and record maintenance documentation performed on Health Care electronic information resources.

b. Standard: Workstation Security. Physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users. Access to workstations is controlled in each area by workstation placement to restrict physical accessibility. If workstations must be left in areas unattended by staff that area must be locked to access.

   1. Time-out – Workstations should be configured so that after a period of inactivity, the workstation will automatically log-off requiring the user to log in again to utilize the workstation.

   2. Local storage of restricted information on workstation hard drives is prohibited.

c. Standard: Device and Media Controls. The receipt, utilization and removal of workstations, 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 are governed by the following policies:

   1. Only University issued or HAIS approved computer or mobile devices are permitted to access the UCI HS Network.
2. All UC Irvine Healthcare issued computers or portable computing and electronic storage devices must be returned to UC Irvine when the workforce member leaves the University.

3. Media Disposal (Required). In the event any workstation or computing device containing PHI is not to be reused the media must be sanitized as per industry standards prior to disposal. The allowable method for Media Sanitization is described as per university policy.

(See UC Business and Finance Bulletin RMP-2, Records retention and disposition for disposal processes and guidelines).

4. Media Re-Use (Required). In the event any workstation or computing device containing PHI will be reused the media must be sanitized prior to reuse of that media. The allowable method for Media Sanitization is described as per university policy.

(See UC Business and Finance Bulletin RMP-2, Records retention and disposition for disposal processes and guidelines).

5. Accountability (Addressable). HAIS Support staff will document and maintain a record of the movements of hardware and electronic media. This record is maintained in the Altiris Asset management system and will include the name of the users and HAIS technical staff associated with each relocation.

6. Data Backup and Storage (Addressable). When possible, files containing restricted information must be stored on network shared drives secured by HAIS rather than locally on devices. Storage of electronic files containing unencrypted restricted information on local device drives is not permitted.

7. If local storage of restricted information cannot be technically avoided, a retrievable, exact copy of the information, when needed, should be captured before movement of equipment.

VII. **PROCEDURES**

<table>
<thead>
<tr>
<th>RESPONSIBLE PERSON(S)/DEPT</th>
<th>1 PROCEDURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Proprietors/</td>
<td>A. System Information Security Assessment</td>
</tr>
<tr>
<td>System</td>
<td>The System Proprietor (or System Custodian on behalf of the System Proprietor) will have the following responsibilities:</td>
</tr>
<tr>
<td>Custodians/ System Administrators</td>
<td>1. Will identify systems belonging to the System Owner that contain ePHI or other restricted information.</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>2. Will assist HAIS in performing the information system assessment for systems containing restricted information that belong to the System Owner. (See Health Care Information Services department policy “Information System Risk Assessment” for details)</td>
</tr>
<tr>
<td></td>
<td>3. Will review and communicate the results of the information system assessment and obtain the approval of the Department Administrator or Chief Administrative Officer for any remediation plans.</td>
</tr>
<tr>
<td></td>
<td>4. Will implement, when possible, appropriate internal and security controls that are identified and recommended in the Information Security Assessment (see C. Remediation – below).</td>
</tr>
<tr>
<td></td>
<td>5. On an ongoing basis, will maintain the System in accordance with the recommendation derived from the Information Security Assessment.</td>
</tr>
<tr>
<td></td>
<td>6. Will protect from disclosure any data or report files from the System Information Security Assessment. Electronic files from the assessment should only be stored on secure network servers.</td>
</tr>
<tr>
<td>Information Security Team (IST)</td>
<td>B. System Information Security Assessment -</td>
</tr>
<tr>
<td></td>
<td>1. The IST and designees will assist the System Owners/System Administrators with the technical and data collection details, as needed, to complete the Risk Assessment.</td>
</tr>
<tr>
<td></td>
<td>2. Risk Assessment Report –</td>
</tr>
<tr>
<td></td>
<td>a. The IST will provide the System Owners / System Administrators and their Department Administrator or Chief Administrative Officer the System Risk Assessment result documentation with the control recommendations.</td>
</tr>
<tr>
<td></td>
<td>b. The System Risk Assessment Report is reviewed and approved as appropriate by a consensus of the IST.</td>
</tr>
<tr>
<td></td>
<td>c. The IST will store, in a secure network environment database, data collected and reports generated from all risk assessments. The information generated from the Risk Assessment process is confidential and must be protected from unauthorized disclosure to prevent security risks.</td>
</tr>
<tr>
<td></td>
<td>d. The report and or report summaries will be available to the UC Irvine Senior Management, Privacy and Security Governing Board and UCOP as requested.</td>
</tr>
<tr>
<td>System Proprietor/ System Administrators/</td>
<td>1. System information security risk remediation and control recommendations are provided in the Risk Assessment report. HAIS will assist the System Proprietors, System Custodians, System Administrators in developing a risk remediation and implementation plan as discerned from the assessment report.</td>
</tr>
<tr>
<td>HAIS / IST</td>
<td>2. System Proprietors, System Custodians, System Administrators, with the assistance of IST will be responsible for providing a remediation completion report to the Security Officer or designee. The IST will document the remediation completion in the Risk Assessment database.</td>
</tr>
<tr>
<td>Senior Management</td>
<td>3. Technical security standards and control recommendations for which the cost is prohibitive to implement or technically impossible to implement must be addressed with alternate security precautions to minimize risk to ePHI or other restricted information.</td>
</tr>
<tr>
<td></td>
<td>a. Alternate security precautions must be documented including:</td>
</tr>
<tr>
<td></td>
<td>i) The rationale for the decision to implement the alternate safeguard,</td>
</tr>
<tr>
<td></td>
<td>ii) Details of the alternate safeguard implemented; and</td>
</tr>
<tr>
<td></td>
<td>iii) Any future plans for achieving compliance with the technical standard.</td>
</tr>
<tr>
<td></td>
<td>4. In the event the System Proprietors, System Custodians, System Administrators are unable to execute the remediation recommendations, due to financial or other reasons, the Senior Management will be informed. It is the responsibility Senior Management to provide guidance or the means necessary to execute the recommendations or to accept the risk as stated.</td>
</tr>
<tr>
<td>System Proprietors/ System Custodians/ IST</td>
<td>C. Time Schedule for System Information Security Assessment and re-assessment</td>
</tr>
<tr>
<td></td>
<td>1. System owners or departments administrators intending to acquire a new or replacement system that support the storage, transmission, or processing of restricted information must notify the IST prior to system purchase and acquisition so that a system risk assessment can be performed. Activation of a new system is contingent upon completion of the risk assessment.</td>
</tr>
</tbody>
</table>
2. System Information Security Assessment will be repeated on a 3 year cycle, or whenever there have been changes that alter system security control measures.

VIII. REFERENCES

University of California Irvine Health Affairs Policy
HIPAA. Privacy Security Breach Notification General Administrative Policy

University of California Irvine Health Affairs Policy
INCIDENT REPORTING, AUTOMATED General Administrative Policy

University of California Irvine Administrative Policy 800-17 UCI Guidelines for Notification in Instances of Security Breaches Involving Personal Information Data

University of California Business and Finance Bulletin, IS-3 Electronic Information Security

University of California Business and Finance Bulletin, RMP-2 Records retention and disposition: principles, processes, and guidelines

Health Insurance Portability and Accountability Act (HIPAA) 45 CFR Parts 160, 162, and 164

Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. S1232g; 34 CFR Part 99)

Gramm-Leach-Bliley Act (GLBA)


Information Security management Understanding ISO 17799
Related Documents

Laws that influence and affect this policy include but are not limited to:

- COPPA  http://www.ftc.gov/coppa/
- ECPA  http://www.access.gpo.gov/uscode/title18/parti_chapter119_.html
- GLBA  http://www.ftc.gov/privacy/glbact/
- HIPAA  http://www.hhs.gov/ocr/hipaa/
- USA Patriot Act  http://www.lifeandliberty.gov/

ORIGINAL ADOPTION & PRIOR REVISION DATES:

Policy Owner(s):  Jeff Barnes  6/6/2011
Information Security Officer

Approvals:

Privacy & Security Policy Committee  07/13/2012
Governing Body  July 23, 2012