Guidelines for HIPAA Security Rule Compliance
University of California

1. INTRODUCTION

This document is intended to assist UC campus and medical center directors and managers to determine the implementation of practices to achieve compliance with the HIPAA Security Rule. Recommendations are consistent with UC IT security policy and generally accepted information security practices. Security Rule standards and specifications are referenced for each recommendation.

This guidance seeks to establish the minimally acceptable practices necessary to comply with both addressable and required standards of the HIPAA Security Rule. The HIPAA standards are intended by the federal government to be both flexible and scalable for large sophisticated users and small operations. Since the University is a large and diverse covered entity, it is not possible to make assumptions about systems which may range from a laptop to a mainframe, from a small branch of student health services to a major medical center. Even some very complex hospital systems are legacies from an earlier era in which current security concerns were not considered. These legacy systems may not be able to meet all current security standards and alternative approaches will need to be implemented. This guidance aims to encompass the diversity at UC while at the same time to establish high standards for the protection of sensitive information.

2. UNIVERSITY POLICY

University policy specifically defines how confidential information should be managed and these recommendations are in agreement with HIPAA since both policy statements are based on the same generally accepted information security principles (GAISP). **Business and Finance Bulletin IS-3, Electronic Information Security** establishes broad guidelines for University compliance with federal and state law, and includes standard professional information technology security recommendations. The provisions in BFB IS-3 address the general policy requirements specified by HIPAA. IS-3 does not contain specific procedural recommendations; these must be determined individually by each campus implementation.

Access to protected data is governed by state and federal laws, both in terms protection of and disclosure of data about individuals. For discussion of what constitutes personal data, see **BFB RMP-8, Privacy and Access to Information about Individuals.**

The Electronic Communications Policy (ECP) clarifies the principles of academic freedom, shared governance, freedom of speech, and privacy as they relate to electronic communications. The ECP establishes a high standard for the nonconsensual access to individual's electronic communications and requires that each campus establish implementation guidelines to ensure compliance with its provisions.

3. HIPAA SECURITY RULE

In April 2003 the University completed a major effort to achieve compliance with the Privacy Rule (45 CFR Parts 160 and 164) implementing the Health Insurance Portability and Accountability Act (HIPAA) of 1996. The focus of the Privacy Rule was the management of protected health information (PHI).

By April 20, 2005 all covered entities must be compliant with the Security Rule (45 CFR Parts 160, 162 and 164). The Security Rule covers electronic creation, transfer, storage and receipt of PHI (ePHI) and was issued in its final form in April 2003.

The University is considered a hybrid covered entity under this regulation, which essentially means that as an organization the University is involved in health care along with other completely separate functions.

HIPAA defines electronic protected health information (ePHI) as 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 that identifies the individual. The definition of PHI in the Privacy and Security Rule excludes education records covered by FERPA and employment records held by UC in its role as employer

Implementation specifications are *required* or *addressable*. A covered entity must implement the *required* implementation specifications. For *addressable* implementation specifications, the following options are available:

i) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity's electronic protected health information;

(ii) As applicable to the entity

(A) Implement the implementation specification if reasonable and appropriate; or

(B) If implementing the implementation specification is not reasonable and appropriate

(1) Document why it would not be reasonable and appropriate to implement the implementation specification; and

(2) Implement an equivalent alternative measure if reasonable and appropriate.

References to standards and specification in the following recommendations will indicate if the specification is required (R) or addressable (A).

HIPAA requires that a security official be assigned responsibility for HIPAA security implementation. On February 7, 2005 Sr Vice President Mullinix requested that campuses, laboratories, and hospitals appoint a HIPAA Security Officer. This individual should work closely with the systemwide taskforce under the direction of the designated University's HIPAA Privacy and Security officer to ensure consistent compliance for the University (§164.308.a.2).

Every campus and medical center must implement policies and procedures consistent with UC's systemwide guidelines to prevent, detect, contain, and correct security violations (§164.308.a.1). Every campus and medical center must oversee a survey of all uses and locations of ePHI and make recommendations to preserve its confidentiality, integrity and availability. Every campus and medical center will establish a clear process for reporting of suspected security incidents, and for incident handling, including documentation, determination of notification requirements, remediation, and reporting to management (§164.308.a.6)(R).

See Appendix A for the complete list of HIPAA Security Rule standards and implementation specifications.

4. RECOMMENDED PRACTICES

Index of Topics

The following list identifies all the practices that should be implemented. Section 5, Considerations for Technical Solutions, provides discussion regarding selected technical solutions.

A. Workforce Identity and Account Management
B. Information Management
C. Continuity Planning and Disaster Recovery
D. Electronic Mail
E. Data Centers
F. Remote Access
G. Information for Users

A. Workforce Identity and Account Management

1. Determine which individuals are authorized to work with ePHI in accordance with a role-based access approach (§164.308.a.3)(A).
2. Establish security training for all members of the UC workforce who are involved in the creation, transmission, and storage of ePHI. Ensure that training program includes periodic security

reminders and is updated to take into account current vulnerabilities and threats. (§164.308.a.5)(A).

3. Take disciplinary action in accordance with University personnel policies and guidelines on workforce members who fail to comply with University policy and procedures, including information security policy and procedures. (See Personnel Policies for UC Staff Members.) (§164.308.a.1)(R).
4. Ensure the verification of the individual or entity who is authorized to access ePHI and that the identity is correctly bound to a unique user identification ("sign-on") for access to ePHI (§164.308.a.4)(A) (§164.312.a.1)(R) (§164.312.d).
5. Ensure appropriate access controls mechanisms for authorized users' access to any ePHI. For systems with the capability, require strong electronic authentication, such as sufficiently complex passwords or use of other encryption key mechanisms to access systems containing ePHI (§164.308.a.5)(A).
6. Establish account maintenance procedures that ensure termination of accounts or change in access privileges for individuals or entities who have terminated or no longer are authorized to access ePHI (§164.308.a.4)(A).
7. Carefully manage system administrator accounts to ensure the accounts are used for only specific system administration functions. The number of these accounts should be kept to a minimum and provided only to personnel authorized to perform identified functions. Passwords or other authentication measures should be changed upon the termination of systems personnel who accessed these accounts.
8. Log activities performed by system administrator accounts and monitor logs on a regular basis (§164.308.a.1)(R) (§164.308.a.5)(A).

B. Information Management

1. Identify relevant information systems (§164.308.a.1)(R).
2. Ensure that agreements with third parties contain language that University ePHI receive appropriate safeguards (§164.308.b.1)(R Identify relevant information systems (§164.308.a.1)(R).
3. Conduct risk assessments to identify the electronic information resources that require protection, and to understand and document risks from security failures that may cause loss of confidentiality, integrity, or availability. Risk assessments should take into account the potential adverse impact on the University's reputation, operations, and assets (§164.308.a.1)(R). Risk assessments should include analysis of scenarios that may result in modification of ePHI by unauthorized sources (§164.312.c.1)(A).
4. Select appropriate mechanisms to safeguard data relative to the sensitivity or criticality determined by the risk assessment (§164.308.a.1)(R). Procedures should address risks to integrity of ePHI resulting from unauthorized access (§164.312.c.1)(A).
    - Systems containing ePHI need to be hardened against known operating system vulnerabilities.
    - Where appropriate, install firewalls and intrusion detection software to reduce threat of unauthorized remote access (§164.308.a.5)(A).
    - Protect sensitive data with appropriate strategies, such as removal of restricted data from data sets (de-identification), secure file transfer, and use of web browser security standards, virtual private networks, and encryption (§164.312.a.1)(A).
    - Protect all devices against malicious software, such as computer viruses, Trojan horses, spyware, etc. (§164.308.a.5)(A).
    - Use change management practices for systems containing ePHI.
    - Run versions of operating system and application software for which security patches are made available and installed in a timely manner on networked devices.
5. Implement procedures to ensure regular review of log-in attempts and system activity, including the report of discrepancies (§164.308.a.1)(R) (§164.308.a.5)(A).
6. Where possible, terminate electronic sessions after a period of inactivity (§164.312.a.1)(A).
7. Thoroughly scrub all ePHI from any storage media prior to disposal or re-use (§164.310.d.1)(R).

8. Implement appropriate logical security measures, such as encryption, to protect data from unauthorized access if systems or work-stations containing ePHI cannot be housed in a professionally-managed secure location, i.e., data centers (§164.312.e.2)(A).
9. Conduct back up of data and software on an established schedule. Back up copies should be stored in a physically separate location from the data source (§164.308.a.7)(R).

C. Continuity Planning and Disaster Recovery

1. Ensure that business continuity planning includes measures to enable continuation of critical business processes while operating in emergency mode and to recover from a disaster that renders resources unavailable for an acceptable period of time. Disaster recovery plans must be tested on a periodic basis or in response to major changes to the working environment (§164.308.a.7)(R).
2. Continuity plans must undergo periodic testing and revised as appropriate (§164.308.a.7)(A).
3. Establish procedures to ensure that ePHI can be accessed during an emergency (§164.312.a.2)(R).

D. Electronic Mail

1. Educate staff about the risks of email and adopt programs to educate staff regarding appropriate use of email.
2. All confidential email must be sent via secure channels.
3. Alert patients to the risks of unsecured email.
4. Consider alternative secure email/web messaging solutions for direct patient communication (§164.312.e.1)(A).
5. Whenever deemed necessary and possible encrypt transmissions containing ePHI (§164.312.e.1)(A).

E. Data Centers

1. Data centers that contain ePHI should be located in professionally-managed secure locations that have provisions for prevention, detection, early warning of, and recovery from emergency conditions created by earthquake, fire, water leakage or flooding, power disruption, air conditioning failures, or other hazards (§164.310.a.1)(A).
2. These secure locations must have physical access controls, such as locks, electronic key readers, or other access control mechanisms (§164.310.a.1)(A).
3. Record any maintenance repairs and modifications to physical components of the facility related to security, such as hardware, walls, doors, and locks (§164.310.a.1)(A).
4. Record relocation of hardware and electronic media. Assign responsibility for maintaining records of hardware and software (§164.310.d.1)(A).
5. Limit access to secure locations to authorized users only, and maintain logs to track ingress and egress from location (§164.310.a.1)(A).
6. Ensure back up of data before the relocation of equipment (§164.310.d.1)(A).

F. Remote Access

1. All remote access into UC networks must be by secure methods only, such as authorized VPNs (§164.312.e.1)(A).
2. Storage of ePHI on any non university equipment is forbidden unless formal exemption granted following assessment of the risks.
3. Since laptops can never be adequately secured physically the best protection is encryption which would render the laptop contents undecipherable to unauthorized users (§164.312.e.1)(A)..

G. Information for Users

1. All members of the UC workforce who are involved in the creation, transmission and storage of ePHI must receive training about the HIPAA security rule.
2. Access to ePHI is limited to those individuals for whom it is an authorized work related requirement.
3. You may be subject to disciplinary action in accordance with University personnel policies and guidelines on workforce members who fail to comply with departmental security policy and procedures. In other words misuse or unauthorized access of ePHI may be subject to sanction and disciplinary actions.
4. You must use a sufficiently complex passwords to access systems containing ePHI. This password must never be shared. Passwords should be developed in accordance to policies set forth by your campus information technology (IT) services.
5. You must run versions of operating system(s) and application software for which security patches are made available and installed in a timely manner.
6. All devices must be protected against malicious software, such as computer viruses, Trojan horses, spyware, etc. Where appropriate, install firewalls and intrusion detection software to reduce threat of unauthorized remote access. This includes servers, workstations. Laptops, tablets, PDAs, smart phones, etc…must be backed up to secure servers if they contain ePHI.
7. Portable devices, such as laptops, if they contain ePHI should be password protected or encrypted, and other logical controls installed, since they cannot be physically secured.
8. All devices which contain ePHI must be backed up on an established schedule.
9. You must secure, maintain and when necessary dispose of all removable electronic media that may contain ePHI according to established procedures. This includes tape drives, tapes, portable hard drives, CD-ROMs, DVDs, floppy disks, USB and flash memory cards.
10. Whenever deemed possible encrypt electronic transmissions containing EPHI (such as email containing ePHI). If encryption is not available, consider email a public document.

5. CONSIDERATIONS FOR TECHNICAL SOLUTIONS

These recommendations are meant to address individual HIPAA standards in which technical solutions are indicated. They are not considered comprehensive responses to the rule and in fact given the very wide range of activities included in the University's covered entity it is not prudent for this group to issue any mandates. Individual units will conduct their own risk assessments and determine mitigations that are commensurate with the assessed risks.

Audit Retention (§164.312 (b))

The rule requires that records be maintained of "activity in information systems that contain or use ePHI". This functionality is included in most modern software programs, in particular the complex databases used in hospitals. Not every UC work environment uses such databases and in those instances maintaining an audit log may not be possible. In cases in which ePHI is contained in systems which lack audit controls other measures such as access controls and confidentiality agreements will be necessary.

In systems that do maintain this information the question is the appropriate period of retention. In the administrative simplification section (§164.316(b)(2)(i) Policies, Procedures and Documentation Requirements - *Time Limit*) the requirement for retention for six years is set forth. It would be prohibitively expensive and probably inefficient to store massive amounts of data for years.

For this reason only logs relevant to security incidents should be retained for six years and the remainder of the data should only be retained for up to 90 days in accordance with usual and customary practice. Periodic audits, whether for cause or not, should be conducted of the information systems so that relevant audit logs can be identified for future review even if no incident has come to light.

Email Encryption: (§164.312(e)(1))

Electronic mail is fundamentally insecure. Email in transit may potentially be viewed by many individuals since it may pass through several switches enroute to its final destination. It may not reach the intended recipient at all. In practice the risks for a single piece of email are extremely small given the volume of email traffic. Nevertheless, emails containing ePHI need to be considered worthy of a higher level of security. The following recommendations are offered to address these concerns:

1. Educate staff and patients about the limitations of email. Any solution will depend on changing staff behavior and attitudes to the use of email.
2. Obtain consent from patients for use of email which outlines the risks of the medium.
3. Employ an integrated messaging solution such as that marketed by RelayHealth. This system is in use at UCDMC and UCIMC for secure doctor-patient communication
4. Implement an email encryption program such as Tumbleweed, Zixmail and others and train staff how to use appropriately.

Patch Management (§164.308(a)(5))

Protection from security breaches in large part depends on computing system maintenance. Software vendors regularly provide updates or patches so that their products continue to be valuable to their customers. Ensuring that all available and relevant patches are installed is an ongoing and complicated activity. In addition maintaining anti-virus and anti-spyware programs is a continuous challenge. In most network environments the managers can ensure that computers on the network are running the correct versions and have installed patches. Computers that may not be on the network such as laptops and PDAs will require more active surveillance and maintenance by the individual users. For example see UCOP, Managed Desktop Initiative.

Physical Security (§164.310(a)(1))

Data must be available when needed but its integrity must be maintained. Access to systems containing ePHI must be controlled as carefully as possible. In addition to malicious software there are significant physical risks to these assets. In particular computers which are housed in leased property or which are accessed by contract cleaning and maintenance services need to be carefully secured. Record any maintenance repairs and modifications to physical components of the facility related to security, such as hardware, walls, doors, drop ceilings and locks. Limit access to secure locations to authorized users only, and maintain logs to track ingress and egress from location.

Servers containing ePHI should be housed in professionally-managed secure locations that have provisions for prevention, detection, early warning of, and recovery from emergency conditions created by earthquake, fire, water leakage or flooding, power disruption, air conditioning failures, or other hazards. Secure locations must have physical access controls, such as locks, electronic key readers, or other access control mechanisms Physical security is very often difficult to maintain in unsupervised open areas. Desktops and laptops are by definition not housed in secure areas so ePHI should not be stored on desktops or laptops if a network server is available. Wireless networks pose an additional physical risk insofar as the access points can be compromised and by definition microwave signals are not confined by walls. Wireless signals should be encrypted and access points hidden.

Backing Up/Contingency Plans (§164.308(a)(7))

Any equipment containing ePHI should be regularly backed up to preserve the availability and integrity of the data. Contingency plans for a disaster should take into account the need to restore data in a rational manner. Adequate contingency planning would be based on the criticality of the data, how frequently it is accessed and how quickly it is needed. Paper backup methods should be devised if appropriate. The availability of equipment to which to restore lost data must also be assessed. Back up strategies should take into account not only disaster recovery needs, but also routine departmental workstation or system back up needs. Damage to systems can be widespread and therefore machines and data for recovery purposes must be in physically separate locations. If this is not possible then use of equipment such as fireproof safes are recommended. Replacement equipment can be drop shipped on a pre-arranged basis. Data stored on mobile devices should be considered so vulnerable that the essential contingency plan for such data should be the presumption that it will be lost at some point.

Remote Access

Use of portable devices and home computers to access ePHI remotely is inherently problematic and requires creative solutions within a framework of strict access controls. Storage of ePHI on any home computer is strongly discouraged. Since laptops can never be adequately secured physically the best protection is data encryption which would render the laptop contents undecipherable to unauthorized users. PDAs should be set up to require login that cannot be disabled by the user (set at the server level). All data on PDAs should be regularly synchronized with servers so that if a PDA equipped with login is lost or the password is lost then no data will be recoverable. Some devices such as the Blackberry™ can be set to permit only 10 login attempts before erasing all data. Publicly accessible computers, open wireless networks and third party proxy services (Yahoo!, Hotmail, etc…) are all very vulnerable to penetration by malicious software and hackers and access to ePHI via such systems should be discouraged strongly. Virtual Private Networks (VPN) should be required. Along with this requirement comes the obligation to maintain security patches at remote locations.

Password Management

Passwords are one of the most universal and widely distributed forms of computer security, without individual and sufficiently complex passwords systems containing ePHI cannot be secured. While some legacy systems may not support strong passwords most modern systems can do so. Strong passwords include numbers, symbols and letters of different cases. Since these type of passwords can be difficult to recall the use of a passphrase acronym is advisable. Biometric identification devices and token based systems should be seriously considered as they become available, viable and cost effective.

Access Control

Access to ePHI is considered from many perspectives in the Security Rule. From the technical perspective one prominent issue is emergency access to systems during disasters or other problems requiring temporary access by managers who need to override privileges. This is referred to as a “fire ID”. Systems should be designed to provide single us passwords which are replaced daily and their use tracked closely. Certainly there will need to be exceptions made for access to ePHI to provide patient care in disasters that may outstrip the ability to provide temporary passwords and measures should be in place to ensure that once the need has passed the expanded access granted is rescinded.

Automatic Logoff

Many pieces of equipment and some software programs are designed to log users off after a pre-determined period of inactivity. Either hardware or software logoff systems are adequate. Proximity based logoff systems may become available and cost effective in the future. Such systems would use a proximity card reader to determine whether the user is physically adjacent and thereby active.

Termination Procedures

Employee termination often leaves ePHI access unencumbered. This is no longer acceptable for even a brief period under the HIPAA Security Rule. Payroll systems which can automatically prompt IT services to terminate access are ideal.

APPENDIX A—HIPAA SECURITY RULE

Paragraph	**Standards** **Implementation Specifications**
§164.308	**ADMINISTRATIVE SAFEGUARDS**
§164.308(a)	A coverend entity must, in accordance with §164.306:
§164.308(a)(1)(i)	***Security management process*** Implement policies and procedures to prevent, detect, contain, and correct security violations.
§164.308(a)(1)(ii)(A)	**Risk analysis *(Required)*** Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.
§164.308(a)(1)(ii)(B)	**Risk management *(Required)*** Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.308(a).
§164.308(a)(1)(ii)(C)	**Sanction policy *(Required)*** Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.
§164.308(a)(1)(ii)(D)	**Information system activity review *(Required)*** Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
§164.308(a)(2)	***Assigned security responsibility*** Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.
§164.308(a)(3)(i)	***Workforce security*** Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a) (4) of this section, and to prevent those workforce members who do not have access under paragraph (a) (4) of this section from obtaining access to electronic protected health information.
§164.308(a)(3)(ii)(A)	**Authorization and/or supervision *(Addressable)*** Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

§164.308(a)(3)(ii)(B) **Workforce clearance procedure *(Addressable)***
Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

§164.308(a)(3)(ii)(C) **Termination procedures *(Addressable)***
Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a) (3) (ii) (B) of this section.

§164.308(a)(4)(i) ***Information access management***
Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

§164.308(a)(4)(ii)(A) **Isolating health care clearinghouse functions *(Required)***
If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

§164.308(a)(4)(ii)(B) **Access authorization *(Addressable)***
Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

§164.308(a)(4)(ii)(C) **Access establishment and modification *(Addressable)***
Implement policies and procedures that, based upon the entity’s access authorization policies, establish, document, review, and modify a user’s right of access to a workstation, transaction, program, or process.

§164.308(a)(5)(i) ***Security awareness and training***
Implement a security awareness and training program for all members of its workforce (including management).

§164.308(a)(5)(ii)(A) **Security reminders *(Addressable)***
Periodic security updates.

§164.308(a)(5)(ii)(B) **Protection from malicious software *(Addressable)***
Procedures for guarding against, detecting, and reporting malicious software.

§164.308(a)(5)(ii)(C) **Log-in monitoring *(Addressable)***
Procedures for monitoring log-in attempts and reporting discrepancies.

§164.308(a)(5)(ii)(D) **Password management *(Addressable)***
Procedures for creating, changing, and safeguarding passwords.

§164.308(a)(6)(i) ***Security incident procedures***

Implement policies and procedures to address security incidents.”

§164.308(a)(6)(ii) **Implementation specification: Response and Reporting *(Required)***
Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

§164.308(a)(7)(i) ***Contingency plan***
Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

§164.308(a)(7)(ii)(A) **Data backup plan *(Required)***

Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

§164.308(a)(7)(ii)(B) **Disaster recovery plan *(Required)***
Establish (and implement as needed) procedures to restore any loss of data.

§164.308(a)(7)(ii)(C) **Emergency mode operation plan *(Required)***
Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

§164.308(a)(7)(ii)(D) **Testing and revision procedures *(Addressable)***
Implement procedures for periodic testing and revision of contingency plans.

§164.308(a)(7)(ii)(E) **Applications and data criticality analysis *(Addressable)***
Assess the relative criticality of specific applications and data in support of other contingency plan components.

§164.308(a)(8) ***Evaluation***
Perform a periodic technical and nontechnical evaluation, based initially upon the standards and 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 this subpart.

§164.308(b)(1) ***Business associate contracts and other arrangements***
A covered entity, in accordance with §164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity’s behalf only if the covered entity obtains satisfactory assurances, in accordance with §164.314(a) that the business associate will appropriately safeguard the information.

§164.308(b)(4) **Written contract or other arrangement (*Required*)**

Document the satisfactory assurances requried by paragraph (b)1 of this section through a written contract or other arrangement with the business associate that meets the applicaqble requirements of §164.314(a).

§164.310 PHYSICAL SAFEGUARDS

§164.310(a) A coverend entity must, in accordance with §164.306:

§164.310(a)(1) **Facility access controls**

Implement policies and procedures 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.

§164.310(a)(1)(i) **Contingency Operations *(Addressable)***

Establish (and implement as needed) 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.

§164.310(a)(1)(ii) **Facility security plan *(Addressable)***

Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

§164.310(a)(1)(iii) **Access control and validation procedures *(Addressable)***

Implement procedures 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.

§164.310(a)(1)(iv) **Maintenance records *(Addressable)***

Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

§164.310(b) ***Workstation use***

Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

§164.310(c) ***Workstation security***

Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

§164.310(d)(1) ***Device and media controls***

Implement policies and procedures that govern the receipt and removal of 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.

§164.310(d)(2)(i) **Disposal *(Required)***

Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.

§164.310(d)(2)(ii) **Media re-use *(Required)***

Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.

§164.310(d)(2)(iii) **Accountability *(Addressable)***

Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

§164.310(d)(2)(iv) **Data backup and storage *(Addressable)***

Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

§164.312 TECHNICAL SAFEGUARDS

§164.312(a) A coverend entity must, in accordance with §164.306:

§164.312(a)(1) ***Access Control***

Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).

§164.312(a)(2)(i) **Unique user identification *(Required)***

Assign a unique name and/or number for identifying and tracking user identity.

§164.312(a)(2)(ii) **Emergency access procedure *(Required)***

Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

§164.312(a)(2)(iii) **Automatic logoff *(Addressable)***

Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

§164.312(a)(2)(iv) **Encryption and decryption *(Addressable)***

Implement a mechanism to encrypt and decrypt electronic protected health information.

§164.312(b) ***Audit controls***

Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

§164.312(c)(1) ***Integrity***

Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

§164.312(c)(2) **Mechanism to authenticate electronic protected health information *(Addressable)***

Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

§164.312(d) ***Person or entity authentication***

Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

§164.312(e)(1) ***Transmission Security***

Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

§164.312(e)(2)(i) **Integrity controls *(Addressable)***

Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

§164.312(e)(2)(ii) **Encryption *(Addressable)***

Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.