County of Sacramento

Health Insurance Portability and Accountability Act (HIPAA)

SECURITY RULE
POLICIES AND PROCEDURES

Issued: February 1, 2005
Effective: April 14, 2005
Revised: February 29, 2016

HIPAA Security Officer: Rami Zakaria
HIPAA Privacy Officer: Donna Allred

Office of Compliance
799 G Street, Suite 217
Sacramento, CA 95814
(916) 874-2999
www.inside.compliance.saccounty.net

(This page is intentionally blank)

Table of Contents

(This page is intentionally blank)

Definitions

Terms	Definitions
Business Associate	A contractor who completes a function or activity involving the use or disclosure of protected health information (PHI) or electronic protected health information (EPHI) on behalf of a HIPAA covered component. Services that Business Associate (BA) contractors provide include: claims processing or administration; data analysis, processing and/or administration; utilization review; quality assurance; billing; benefit management; document destruction; temporary administrative support; legal; actuarial; accounting; consulting; information technology (IT) support. The BA contractor does not deliver health care services to clients of the HIPAA covered component.
Cloud (private cloud)	A cloud computing platform that is implemented within the corporate firewall, under the control of the IT department.
Covered component	For the purposes of this policy, each department covered by the HIPAA Security Rule is one covered component. The County's HIPAA covered components include Department of Health and Human Services, Department of Behavioral Health Services, Personnel Services–Employee Benefits Office, County Counsel, Countywide Services Agency in the County Executive Office, Department of Revenue Recovery and the Office of Compliance.
Device	A device is a unit of hardware, inside or outside the case or housing for the essential computer functions (the processor, memory, and data paths). A device is capable of providing input, receiving output, or both.
Dial up	Dialing in to an internet service provider over a modem and phone line.
Disposal	The removal or destruction of electronic protected health information from electronic media.
Electronic Protected Health Information (EPHI)	**Electronic** Information in electronic format such as: information system applications; internet, intranet and extranet; email; USB drives; computer screens; laptops; storage devices (magnetic tapes, floppy disks, CDs, optical devices) **Protected Health Information (PHI)** PHI is health information that a covered entity creates or receives that identifies an individual, and relates to: • The individual's past, present, or future physical or mental health or condition;

Terms	Definitions
	• The provision of health care to the individual; or • The past, present, or future payment for the provision of health care to the individual. **Exceptions: PHI and/or EPHI does not include the following:** • Education records • Workman's Compensation records • Health information in workforce member personnel records
Encryption	A method of scrambling or encoding electronic data to prevent unauthorized access. Only individuals with access to a password or key can decrypt (unscramble) and use the data.
Facility	A County owned or leased building in which the workforce accesses Protected Health Information (PHI) or Electronic Protected Health Information (EPHI).
Firewalls	Software or hardware to prevent an intruder from stealing or destroying data.
Hard drive	An information storage device that contains electronic information and software programs on a computer. Information stored on the hard drive [or local (C:) drive] is not backed up on the County's network.
IT	Information Technology. Refers to the Department of Technology (DTech).
Key pads – cipher locks	Door locks that require a combination of numbers entered into a pad in order to unlock the door.
Local (C:) drive	In the context of this policy, this is the individual user's hard drive where electronic information can be stored (saved), rather than stored on the organization-wide network. The local (C:) drive should not be used to store EPHI.
Malicious software or malware	A type of software that includes ways of attacking data integrity, the system itself or the confidentiality of the data. Malicious software includes viruses, virus variants, worms, hoaxes, and Trojan horses.
Media reuse	A device such as a computer hard drive that contained data (information) that is being reused to contain new data.
Modem	A device that enables data to be transmitted over telephone or cable lines. It translates telephone tones to allow for the multiplexing of data (information) across the telephone network, generally in order to access the internet.
Network	A group of computers (workstations) and associated devices connected by a communications channel to share information

Terms	Definitions
	files and other resources between multiple workforce members.
Network closets	Storage area of network equipment such as hubs, routers, switches, racks, cables, and sometimes has telephone equipment, at a HIPAA covered component facility.
Networked computer / workstation	A workstation computer that uses server resources. It is usually connected to a Local Area Network (LAN), which shares the resources of one or more large computers.
Payload	Harmful code delivered by a software virus.
Perimeter security	Security that protects the network and its component server computers from attack or intrusion.
Portable media	Devices carried or moved with ease that can contain electronic protected health information (EPHI). The most common are: laptops; CDs; USB drives (or memory sticks); and smartphones, tablets, or other electronic storage devices.
Risk assessment	A process of assessing those factors that could affect confidentiality, availability, and integrity of key information assets and systems. HIPAA covered components are responsible for ensuring the integrity, confidentiality, and availability of EPHI and equipment that contains it, while minimizing the impact of security procedures and policies upon business productivity.
Security access cards, C-Cure badges	Cards used to gain access to a facility (also known as proximity cards or cardkeys). The credit card-sized card is held up to a reader and acts as an electronic key to unlock a door. A card's ability to unlock a door is limited by the cardholder's access clearance.
Server	A computer or device on a network that managers network resources.
Server Room	The room where all the server computers are housed
Strong passwords	A password that is difficult to guess by both humans and computer programs, effectively protecting data from unauthorized access. A strong password consists of at least six characters that are a combination of letters, numbers and symbols (@, #, $, %, etc.) if allowed. Strong passwords contain the maximum number of characters allowed. Passwords are typically case-sensitive so a strong password contains letters in both uppercase and lowercase. Strong passwords also do not contain words that can be found in a dictionary or any part of the user's own name.
Transmitting	The act of sending a message or data using an electronic medium, including email, electronic (Internet Protocol [IP]) faxing, or other electronic communication.

Terms	Definitions
Trojan or trojan horse	A trojan or trojan horse is a computer program generally designed to impact the security of a network system. The trojan is usually disguised as something else (a benign program) or masquerades as a legitimate file that the user would expect to see, or want to load, on the network system. The payload of a trojan is usually delivered as soon as it is opened with devastating results. Trojans often create “back doors” that allow access into a secure network. A hacker can then gain access to the secure network. Trojans are most often delivered as an attachment to a seemingly innocent chain email.
USB drive, USB flash drive or memory stick	A small, portable device that plugs into a workstation computer’s USB port and functions as a portable hard drive with extra storage capacity. USB devices are easy to use, small enough to be carried in a pocket, and can plug into any workstation computer with a USB drive.
User	For the purposes of this document, the term user refers to any workforce member (permanent or temporary), contractor, consultant, vendor, volunteer, student or other person who uses, maintains, manages or is otherwise given access privileges to County IT systems.
User ID or logon	An identification code issued for access privileges which identifies the user to County IT systems.
Virtual Private Network (VPN)	A secure, encrypted network connection between two or more devices across the public internet or other shared network. It allows workstation computers at different locations to securely communicate with each other.
Virus	A computer program that copies itself into another program, sectors on a drive, or into items that support scripts. A virus may unleash a payload. Payloads can damage files, corrupt hard drives, display messages, or open other files. Typically, the payload is delivered when a certain condition occurs, such as when the date on the workstation reaches a particular day.
Workforce / workforce member	In the HIPAA Privacy Rule, the term "workforce" is defined as "employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a HIPAA covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.” “Employees” include supervisors, managers and staff.
Workstation	A laptop or desktop computer, or any other device that performs computer functions.
Worm	A worm is a type of virus that finds vulnerable computer systems

Terms	Definitions
	and then copies itself into those systems. The most frequent copying methods are from email distribution lists, email signature scripts, and shared folders on the network. A typical worm payload makes the workstation more susceptible to other malicious viruses.

(This page is intentionally blank)

Policy 1: Assigned Security Responsibility

Issue Date: February 2005
Effective Date: April 21, 2005
Revised Date: February 29, 2016

1.1 HIPAA Regulation:

- *Assigned security responsibility*

1.2 Policy Purpose:

At all times the County of Sacramento shall have one individual identified and assigned to HIPAA security responsibility.

1.3 Policy Description:

The HIPAA Security Officer is responsible for the oversight of Security Rule implementation by departments with HIPAA covered components. Responsibilities are:

1. To ensure that the necessary and appropriate HIPAA security policies are developed and implemented to safeguard the integrity, confidentiality, and availability of electronic protected health information (EPHI) within the HIPAA covered components.
2. To ensure that the necessary infrastructure of personnel, procedures and systems is in place through monitoring, compliance, and providing a mechanism for incident reporting and violations.
3. To act as a single point of contact for Sacramento County in all issues related to HIPAA security.

1.4 Policy Responsibilities:

The above HIPAA Security Officer responsibilities are assigned to the Chief Information Security Officer for the County of Sacramento. The current County of Sacramento Information Technology Constitution identifies the Chief Information Officer as the Chief Information Security Officer (CISO).

Historically, the HIPAA Security Officer has delegated assigned responsibilities of the Security Rule implementation to the Office of Compliance.

The Office of Compliance shall coordinate the program level support for the HIPAA Security Rule implementation with the County's HIPAA Deputy Compliance Officers (DCOs), who are assigned by the department directors of the HIPAA covered components.

(This page is intentionally blank)

Policy 2: Policy Documentation

Issue Date: February 2005
Effective Date: April 21, 2005
Revised Date: February 29, 2016

2.1 HIPAA Regulation:

- *Policies and procedures*
- *Documentation*
- *Time limit*
- *Availability*
- *Updates*

2.2 Policy Purpose:

The purpose of this policy is to establish the process by which County of Sacramento HIPAA Security Rule Policies and Procedures are created and maintained in accordance with federal regulations.

2.3 Policy Description:

The County of Sacramento is required to have policies and procedures for compliance with the HIPAA Security Rule.

2.3.1 Policies and Procedures

1. As assigned by the HIPAA Security Officer, the Office of Compliance shall draft new or revised HIPAA Security Rule Policies and Procedures as required due to:
    a. Changes in business practices or the Information Technology (IT) environment of the HIPAA covered components
    b. Mandated federal law enacted by Congress
    c. Risk analysis determines new or increased vulnerability to security threat
2. The County Compliance Officer, who is assigned responsibilities of the HIPAA Privacy Officer, shall direct the Office of Compliance in the revision process, and provide review for compliance standards. Legal review of the policies and procedures will be made by the Office of County Counsel. Approval of the HIPAA Security Rule Policies and Procedures will be made by the County's Chief Information Security Officer who is assigned the responsibilities of the HIPAA Security Officer.
3. All policies and procedures implemented to comply with the HIPAA Security Rule shall be made available to the HIPAA covered component workforce.
4. All actions, activities, or assessments required by the County's HIPAA Security Policies and Procedures shall be documented. The documentation shall provide sufficient detail to communicate the implemented security measures and to facilitate periodic evaluations by the HIPAA covered components or as requested by the County's HIPAA Security Officer.

5. In accordance with 45 CFR §164.316, documentation shall be retained for a minimum of 6 years from the time of its creation or the date it was last in effect, whichever is later.
6. Security procedures developed by the HIPAA covered components shall be consistent with the County HIPAA Security Rule Policies and Procedures.

2.4 Policy Responsibilities:

2.4.1 Office of Compliance Responsibilities

1. Draft new or updated HIPAA Security Rule Policies and Procedures as indicated in **Section 2.3.1**.
2. Communicate the approved new or revised policy to the workforce of the HIPAA covered components, and update training and related materials as needed.
3. Maintain and make available to the workforce the HIPAA Security Rule policies and procedures in electronic form on the County's intranet.

2.4.2 County Compliance Officer/HIPAA Privacy Officer Responsibilities

Direct the Office of Compliance in the revision of the County's HIPAA Security Policies and Procedures and provide review for compliance with mandated standards.

2.4.3 Office of the County Counsel Responsibilities

Provide legal review of the County's HIPAA Security Policies and Procedures for compliance with mandated standards.

2.4.4 Chief Information Security Officer/HIPAA Security Officer Responsibilities

Provide final approval of the County's HIPAA Security Policies and Procedures.

Policy 3: User Access Management

Issue Date: February 2005
Effective Date: April 21, 2005
Revised Date: February 29, 2016

3.1 HIPAA Regulation:

- *Workforce security*
- *Authorization and/or supervision*
- *Workforce clearance procedure*
- *Termination procedures*
- *Information access management*
- *Access authorization*
- *Access establishment and modification*
- *Access control*
- *Integrity*
- *Emergency access procedure*

3.2 Policy Purpose:

The purpose of this policy is to establish rules for authorizing access to the computing network, applications, workstations, and to areas where electronic protected health information (EPHI) is accessible. The HIPAA covered components shall ensure that only workforce members who require access to EPHI for work related activities shall be granted access and when work activities no longer require access, authorization shall be terminated.

In Section 160.103 of the HIPAA Privacy Rule, the "workforce" is defined as "employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate."

3.3 Policy Description:

3.3.1 Management and Access Control

Only the workforce member's manager or an appropriate designee can authorize access to the County's EPHI information systems.

Access to the information system or application may be revoked or suspended, consistent with County policies and practice, if there is evidence that an individual is misusing information or resources. Any individual whose access is revoked or suspended may be subject to disciplinary action or other appropriate corrective measures.

3.3.2 Minimum Necessary Access

Each HIPAA covered component shall ensure that only workforce members who require access to Electronic Protected Health Information (EPHI) are granted access.

Each manager or supervisor is responsible for ensuring that the access to EPHI granted to the workforce member is the minimum necessary access required for each work role and responsibilities.

If the workforce member no longer requires access, it is the responsibility of the manager or appropriate designee to complete the necessary process to terminate access.

3.3.3 Granting Access to EPHI

3.3.3.1 Screen Workforce Members Prior to Access

The manager or designee shall ensure that information access is granted only after first verifying that the access of a workforce member to EPHI is appropriate.

3.3.3.2 Sign Security Acknowledgement

Prior to being issued a User ID or logon account to access any EPHI, each workforce member shall sign the *County of Sacramento's Acknowledgement of Information Security Responsibility* before access is granted to the network or any application that contains EPHI, and thereafter shall comply with all County of Sacramento security policies and procedures.

3.3.3.3 Security Awareness Prior to Getting Access

Before access is granted to any of the various systems or applications that contain EPHI, the manager or appropriate designee shall ensure that workforce members are trained to a minimum standard including:

1. Proper uses and disclosures of the EPHI stored in the systems or application
2. How to properly log on and log off the systems or application
3. Protocols for correcting user errors
4. Instructions on contacting a designated person or help desk when EPHI may have been altered or destroyed in error
5. Reporting a potential or actual security breach

3.3.3.4 Management Approval

Each HIPAA covered component shall implement the following policies and procedures:

1. User IDs or logon accounts can only be assigned with management approval or by an appropriate designee.
2. Managers or their designees are responsible for requesting the appropriate level of access for staff to perform their job function.
3. All requests regarding user IDs or computer system access for workforce members are to be communicated to the appropriate system

administrator. All requests shall be made in writing (which may be in an electronic format).

4. System administrators are required to process only those requests that have been authorized by managers or their appropriate designees.
5. A written or electronic record of the authorized request is to be retained by the system administrator for the period of time the approved user has access, plus a minimum of 1 year.

3.3.4 Granting Access in an Emergency

Management has the authority to grant emergency access for workforce members who have not completed the normal HIPAA access requirements if:

1. Management declares an emergency or is responding to a natural disaster that makes client information security secondary to personnel safety.
2. Management determines that granting immediate access is in the best interest of the client.
3. If emergency access is granted, the manager shall review the impact of emergency access and document the event within 24 hours of it being granted.
4. After the emergency event is over, the user access shall be removed or the workforce member shall complete the normal requirements for being granted access.

3.3.5 Termination or Suspension of Access

Department managers or their designated representatives are responsible for terminating a workforce member's access to EPHI in these circumstances:

1. If management has evidence or reason to believe the individual is using information systems or resources in a manner inconsistent with HIPAA Security Rule policies.
2. If the workforce member or management has reason to believe the user's password has been compromised.
3. If the workforce member resigns, is terminated, suspended, retires, or is away on unapproved leave.
4. If the workforce member's work role changes and system access is no longer justified.

If the workforce member is on leave of absence and the user's system access will not be required for more than three weeks, management shall suspend the user's account until the workforce member returns from their leave of absence.

3.3.6 Modifications to Access

If a workforce member transfers to another program or changes their work role within the same program in a County's HIPAA covered component:

1. The workforce member's new manager or supervisor is responsible for evaluating the member's current access and for requesting new access to EPHI commensurate with the workforce member's new work role and responsibilities.

If a workforce member transfers to another program or department outside of the County's current HIPAA covered components:

1. The workforce member's access to EPHI within his or her current unit shall be terminated as of the date of transfer.
2. The workforce member's new manager or supervisor is responsible for requesting access to EPHI commensurate with the workforce member's new work role and responsibilities.

3.3.7 Ongoing Compliance for Access

In order to ensure that workforce members only have access to EPHI when it is required for their job function, the following actions shall be implemented by all HIPAA covered components:

1. Every new user ID or logon account that has not been used after 30 consecutive calendar days since creation shall be investigated to determine if the workforce member still requires access to the EPHI.
2. At least every six months, Information Technology (IT) teams are required to send managers or appropriate designees:
    a. a list of all workforce members for all applications
    b. a list of workforce members and their access rights for all shared folders that contain EPHI
    c. a list of all workforce members approved for access to Virtual Private Network (VPN)
3. The managers or their designees shall then notify their IT support of any workforce members who no longer require access.

3.4 Policy Responsibilities:

3.4.1 Manager and Supervisor Responsibilities

1. Ensure that the access to EPHI granted to each of their workforce member is the minimum necessary access required for each such workforce member's work role and responsibilities.
2. Request termination of access if the workforce member no longer requires access.
3. Work with Personnel Services to establish a process to immediately contact IT and Facilities Management if a workforce member is being released from probation, suspended, or terminated with cause.
4. Validate new User IDs or logon accounts that are not used within 30 days of creation and provide IT with that information.
5. Review semi-annual user and folder access reports and the VPN access reports prepared by IT support and verify to determine if the workforce members still require access to the EPHI.
6. Ensure members of the workforce have signed the IT security agreement and are properly trained before approving access to EPHI.
7. Follow the appropriate security procedures when granting emergency access with support from IT where required.

3.4.2 IT Support Responsibilities

1. Immediately, upon written notification from a manager or supervisor remove or modify a workforce member's access to EPHI.
2. Provide management with a report that identifies new User IDs or logon accounts not used within 30 days of creation.
3. Provide management with a semi-annual report documenting workers with access to EPHI, and requesting verification that access is still required to fulfill the worker's job functions.
4. When required, support management with the appropriate security procedures for granting emergency access.

3.4.3 Workforce Member Responsibilities

Each user of a system or application that contains EPHI shall:

1. Read and sign the Sacramento County Acknowledgment of Information Security Responsibility and the Sacramento County HIPAA Privacy and Security Policies & Procedures Acknowledgement..
2. Follow all County Information Security policies and requirements.
3. Complete HIPAA Privacy and Security training.
4. Immediately report all security incidents to their supervisor.

(This page is intentionally blank)

Policy 4: Authentication and Password Management

Issue Date: February 2005
Effective Date: April 21, 2005
Revised Date: February 29, 2016

4.1 HIPAA Regulation:

- *Mechanism to authenticate electronic protected health information*
- *Person or entity authentication*
- *Password management*
- *Unique user identification*

4.2 Policy Purpose:

The purpose of this policy is to ensure that County HIPAA covered component workforce members select and secure strong passwords to authenticate their access to information systems containing electronic protected health information (EPHI) and to corroborate that EPHI has not been altered or destroyed in an unauthorized manner.

4.3 Policy Description:

Information systems used to access electronic protected health information (EPHI) shall uniquely identify and authenticate workforce members.

4.3.1 Authentication Standards

The password file on the authenticating server shall be adequately protected and not stored in plaintext (unencrypted).

Network and application systems shall be configured to enforce at a minimum:

1. Automatic password expiration at User ID creation and password reset
2. Automatic password expiration every six months
3. A minimum password length of 8 characters
4. A minimum of five previous passwords that cannot be reused with a User ID

4.3.2 User ID and Password Management

All workforce members are assigned a unique User ID to access the County network and are responsible for creating and maintaining the confidentiality of the password associated with their unique User ID.

Supervisors and managers are required to ensure that the workforce under their supervision understands the user responsibilities for securely managing confidential passwords.

Upon receipt of a User ID, the workforce member assigned the User ID is required to change the password provided by the administrator to a password that only he or she knows. Strong passwords shall be created in order to secure access to EPHI.

Workforce members who suspect that their password has become known by another person shall change their password immediately. Workforce members shall not share

with or reveal their password to anyone, including their supervisor, manager or IT support staff.

All privileged system-level passwords (e.g., root, enable, application administration accounts, etc.) shall be changed, at a minimum, each fiscal quarter.

All passwords are to be treated as sensitive, confidential Sacramento County information. If the workforce member's manager or supervisor requires emergency access to a worker's email or individual network drive, refer to **Section 3.3.4 Granting Access in an Emergency.**

4.3.3 Strong Password Guidelines

Create unique passwords that that use a combination of words, numbers, symbols, and both upper- and lower-case letters. Select strong passwords that have the following characteristics:

1. The password contains at least 6 characters.
2. The password contains both upper and lower case characters.
3. The password contains at least one number or special character, such as @, #, $, %, and &.
4. The password is not so hard to remember that you have to write it down, and is difficult for others to guess.
5. Avoid using dictionary words.
6. Do not choose passwords based upon details that others might know, such as your birth date, your Social Security or phone number, or names of family members.

4.3.4 Mechanism to Authenticate Integrity

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

1. Protect and preserve the integrity of EPHI
2. Automatically record and preserve any change or deletion of any electronically stored medical information.
    a. The record of any change or deletion shall include the identity of the person who accessed and changed the EPHI; the date and time the EPHI was accessed; and the change that was made to the EPHI.

4.4 Policy Responsibilities:

4.4.1 Manager and Supervisor Responsibilities

1. Supervisors and managers shall reinforce secure password use by workforce members.
2. If access to another workforce member's account is required, managers/supervisors shall follow the emergency access procedures in **Section 3.3.4 Granting Access in an Emergency**.

4.4.2 Department IT Support Responsibilities

1. System administrators shall verify the identity and the authority of the workforce member or an authorized requester, such as the member's manager or supervisor, before providing the password for a new User ID.
2. System administrators shall verify the identity and the authority of the workforce member requesting a password reset.
3. System administrators shall verify the identity and the authority of an authorized requester, such as the member's manager or supervisor, to request a password reset for another workforce member.
4. System administrators shall ensure that electronic medical records or medical record systems automatically record and preserve any change or deletion of EPHI, including the identity of the individual(s) making the change; the date and time of the change; and what was changed.

4.4.3 Workforce Member Responsibilities

1. Workforce members shall create and securely manage strong passwords for access to systems containing EPHI.
2. Workforce members shall follow the password protection requirements to protect the confidentiality of their passwords to ensure security of EPHI:
   - Passwords shall not be shared with or revealed to anyone, including their supervisor, manager or IT support staff
   - Passwords shall never be revealed on questionnaires or security forms
   - Passwords shall be memorized, not written down
   - The password used to access the County network shall not be used anywhere else
   - The password shall be changed immediately if the workforce member suspects it has become known by another person
3. Workforce members shall not use another individual's login or password.
4. Workforce members shall report any unauthorized changes of EPHI.

(This page is intentionally blank)

Policy 5: Facility Access Controls

Issue Date: February 2005
Effective Date: April 21, 2005
Revised Date: February 29, 2016

5.1 HIPAA Regulation:

- *Facility security plan*
- *Facility access controls*
- *Access control and validation procedures*
- *Maintenance records*
- *Contingency operations*

5.2 Policy Purpose:

The purpose of this policy is to establish protocols for securing facilities that contain paper protected health information (PHI) and electronic protected health information (EPHI).

5.3 Policy Description:

The County of Sacramento shall reasonably safeguard PHI and EPHI from any intentional or unintentional use or disclosure. The County shall protect its facilities where PHI and EPHI in any form can be accessed.

5.3.1 Facility Security Plan

The County shall safeguard the facilities of its HIPAA covered components and the equipment therein from unauthorized physical access, tampering, and theft.

The Office of Compliance in coordination with the Deputy Compliance Officers shall periodically audit HIPAA covered component facilities to ensure PHI and EPHI safeguards are continuously being maintained.

When designing a new building and remodeling existing sites, facility managers and/or designees shall work with the Office of Compliance to ensure the facility plan components below are compliant with federal HIPAA regulations.

The following shall be implemented for all sites that contain PHI/EPHI:

1. **Access Control:** Authorized workforce members shall receive the facility and/or work site access level appropriate to their work role.
    a. Only authorized workforce members are granted access permission in facilities where protected health information is created or maintained.
2. **Visitor Access Control:** In facilities in which PHI/EPHI is available, all visitors shall be escorted and monitored. Each facility shall implement procedures that govern visitor access controls. These procedures may vary depending on the facility structure, the type of visitors, and where the PHI/EPHI is accessible.

a. Visitors may sign a visitor log that includes the name of the visitor, and time and date of arrival.

b. Patients may be checked in by staff via entry in the electronic medical record in lieu of a visitor log.

c. Only visitors who have a business need shall be admitted into areas in which PHI or EPHI is found.

d. All visitors shall be escorted.

e. Only the workforce member's manager or an appropriate designee (authorized requestor) shall authorize access to facilities or work sites containing PHI or EPHI.

f. Visitors are not left unattended except in public waiting areas.

3. **Security Access Cardkeys:** Facilities that have security access cardkeys (also known as "proximity cards" – a credit card-size card held up to a reader that acts as an electronic key to unlock a door) shall include a card management system and a monitoring system to ensure the appropriate use of the security access cardkeys. When administering security access cardkeys each HIPAA covered component shall have the following:

    a. A standard card format

    b. Defined clearances based on programmatic need, special mandated security requirements and workforce member security

    c. Documentation for the authorization of approved clearances

    d. A back-up procedure in case of system failure

    e. A system for disabling cards when workforce members leave County employment, take an extended leave of absence, discontinue volunteer service, or report their card as lost, missing or stolen

    f. System audits on a semi-annual basis to ensure all workforce members who currently have access continue to require access to the facility

    g. A process to investigate security access cardkeys inactive for 90 days or more to determine if the access cardkey shall be disabled

    h. A tracking mechanism to identify all workforce members with security card access in each facility

4. **Keypads/Cipher Locks:** Facilities shall change the codes on keypads/cipher locks at least every six months in order to ensure the security of staff, property, and the confidentiality of client information. In addition, the facility shall have:

    a. Clearances based on programmatic need, special mandated security requirements and workforce member security, and

    b. A mechanism to track which workforce members are provided access.

5. **Metal/Hard Keys:** Facilities that use metal/hard keys shall change affected or appropriate key locks when keys are lost or a workforce member leaves without returning the key. In addition, the facility shall have:
    a. Clearances based on programmatic need, special mandated security requirements and workforce member security; and
    b. A mechanism to track which workforce members are provided access.
6. **Network Closet(s):** Every network closet shall be locked, whenever the closet is unoccupied or not in use, or shall be enclosed in a locked equipment cage. HIPAA covered components shall maintain a log of who has accessed the network closets and periodically change the locking mechanism to these closets.
7. **Server Room(s):** Every server room shall be locked whenever the room is unoccupied or not in use, or shall be enclosed in a locked equipment cage. HIPAA covered components shall document who has access to each server room and periodically change the locking mechanism to server rooms.
8. **Alarm Systems:** All buildings that contain PHI/EPHI shall have some form of alarm system that is activated during non-business hours. Alarm system codes may only be provided to workforce members who require this information in order to leave and enter a building.
9. **Doors**: All non-public exterior doors (such as employee only doors) and doors leading to areas with PHI/EPHI shall remain locked at all times. It is each workforce member's responsibility to make sure the door that is being entered or exited is completely shut before leaving the door. If a door's closing or locking mechanism is not working, it is every worker's responsibility to notify the facility manager or designee for that facility.

5.3.2 Contingency Operations — Emergency Access to Facilities

Each facility shall have emergency access procedures in place that allow facility access for appropriate workforce members to access PHI/EPHI as well as support restoration of lost PHI/EPHI. This includes a primary contact person and back-up person when facility access is necessary after business hours by persons who do not currently have access to the facility outside of regular business hours.

5.3.3 Maintenance Records

Repairs or modifications to the physical building for each facility where PHI/EPHI can be accessed shall be logged and tracked. The log shall include at a minimum events that are related to security (for example, repairs or modifications of hardware, walls, doors, and locks).

5.4 Policy Responsibilities:

5.4.1 Supervisor and Manager Responsibilities

1. Take appropriate corrective action if any workforce member knowingly violates the facility security plan and its procedures.
2. Authorize clearances that are appropriate to the duties of each workforce member.

3. Notify the Facility Manager or designee within one business day when a user no longer requires access to the facility.
4. Verify that each workforce member surrenders her/his card or key upon leaving employment.
5. Work with the Facility Manager to ensure a log is kept of all access into network closets.
6. Request termination or suspension, as applicable, as soon as possible of access cardkeys that are lost, missing, misplaced, stolen or belong to terminated workforce members.
7. Ensure all staff members responsible for implementing contingency plans have keys, passwords and other information or devices needed to gain access to information system components during emergencies.
8. Review cardkey lists every six months and authorize termination of unused accounts and changes to access levels where applicable.

5.4.2 Workforce Member Responsibilities

1. Display their access/security card or employee badge to demonstrate their authorization to access restricted areas.
2. Do not allow other persons to enter the facility by “tailgating” (entering the facility by walking behind an authorized person through a door without using a valid cardkey in the reader).
3. Do not share access cardkeys, hard keys, alarm codes or keypad codes to enter the facility or areas where there is EPHI.
   a. At all times keep cardkeys, hard keys, alarm codes and keypad codes secured to prevent unauthorized access.
4. Immediately report lost, stolen, missing or misplaced cardkeys, metal keys, keypad-cipher lock codes or alarm codes.
5. Surrender access cardkeys and/or hard key(s) upon leaving employment.
6. Ensure authorized visitors are escorted and not allowed to be unattended in unauthorized areas.

5.4.3 Facility Manager Responsibilities

1. Request and track maintenance repairs.
2. Establish and maintain a mechanism for accessing the facility in an emergency.
3. Track who has access to the facility.
4. Change metal locks when a key is lost or unaccounted for.
5. Change combination keypads/cipher locks every six months.
6. Disable the unique user alarm code when a workforce member is no longer authorized for facility access.
7. Disable access cardkeys not used for 90 days or more.
8. Complete access cardkey audits every 6 months to verify user access.

5.4.4 Office of Compliance and HIPAA Deputy Compliance Officer Responsibilities

1. Work with the Facility Managers of the HIPAA covered components to ensure facilities comply with the HIPAA Security Rule for access controls.
2. Conduct periodic audits of HIPAA covered components to ensure their facilities are secure and the requirements of this policy are enforced.

5.4.5 Department of Technology Responsibilities

1. A written log of who has entered the network closets/server rooms in HIPAA covered components shall be maintained.
2. The locking mechanism to network closets/server rooms within HIPAA covered components that open with a hard key shall be periodically changed.

(This page is intentionally blank)

Policy 6: Workstation Security

Issue Date: February 2005
Effective Date: April 21, 2005
Revised Date: February 29, 2016

6.1 HIPAA Regulation:

- *Access control and validation*
- *Workstation use*
- *Workstation security*
- *Automatic log off*

6.2 Policy Purpose:

The purpose of this policy is to establish rules for securing workstations that access electronic protected health information (EPHI). A workstation is a laptop or desktop computer, or any other device that performs computer functions. Since EPHI can be portable, this policy requires workforce members of HIPAA covered components to protect EPHI at County worksites and all other locations.

6.3 Policy Description:

The County of Sacramento shall implement safeguards to prevent unauthorized access to EHPI through workstations, and to protect EPHI from any intentional or unintentional use or disclosure.

6.3.1 Workstation Security Controls

All workstations used by workforce members of HIPAA covered components to access EPHI shall be set to automatically lock the computer when it is left unattended, requiring the user to enter a password to unlock the workstation. The standard setting for the computer to lock after a period of inactivity is not to exceed 15 minutes, with a recommended inactivity timeout of 5 minutes.

Workforce members shall manually lock their workstation computer when the computer is left unattended for any period of time.

Workforce members shall ensure that observable confidential information is adequately shielded from unauthorized disclosure and access on computer screens. At each site, every effort shall be made to ensure that confidential information on computer screens is not visible to unauthorized persons.

Workforce members who work in other County facilities that are not HIPAA covered components shall be aware of their surroundings to ensure no one can incidentally view EPHI and that no EPHI is left unattended.

Workforce members who work from home or other non-office sites shall follow the above workstation security controls to safeguard EPHI access or viewing by any unauthorized individual.

Workforce members shall protect printed versions of EPHI that have been transmitted via fax or multi-function printers by promptly removing documents from shared devices. Whenever possible, confidential documents are to be placed in locked cabinets or drawers when left unattended.

6.4 Policy Responsibilities:

6.4.1 Supervisor and Manager Responsibilities

1. Control workforce member access to EPHI as per **Security Policy 3: User Access Management.**
2. Take appropriate corrective action if any workforce member knowingly violates the security of workstation use.
3. Ensure that the automatic lock is functioning on all workstations.
4. Ensure that all workforce members are locking their workstations when they are left unattended.
5. Ensure that all confidential information is not viewable by unauthorized persons at workstations in offices under their management.

6.4.2 Workforce Member Responsibilities

1. Lock their computer when it is left unattended for any period of time.
2. Do not change or disable the automatic inactivity lock on their workstation.
3. Ensure that all confidential information in their workstation is not viewable or accessible by unauthorized persons.
4. When working from home, non-HIPAA covered County facilities, or other non-office work sites, protect EPHI from unauthorized access or viewing.

6.4.3 Department of Technology Support Responsibilities

1. When installing new workstations, set the computer to automatically lock after the recommended period of inactivity, which is not to exceed 15 minutes.

Policy 7: Device and Media Controls

Issue Date: February 2005
Effective Date: April 21, 2005
Revised Date: February 29, 2016

7.1 HIPAA Regulation:

- *Device and media controls*
- *Disposal*
- *Media reuse*
- *Accountability*
- *Data backup and storage*

7.2 Policy Purpose:

The purpose of this policy is to ensure that EPHI stored or transported on storage devices and removable media is appropriately controlled and managed. The policy applies to both County issued devices and personal devices that are used to access or store EPHI.

7.3 Policy Description:

7.3.1 Device and Media Protection

Each HIPAA covered component shall protect all the hardware and electronic media that contain EPHI. This includes, but is not limited to, workstation computers, laptops, smartphones, tablets, netbooks, USB drives, backup tapes, and CDs.

Each HIPAA covered component is responsible to develop procedures that govern the receipt and removal of hardware and electronic media that contain EPHI outside of the secured physical perimeter of a County facility, and the movement of these items within the facility. Procedures shall include maintaining a custody record of hardware and electronic media.

7.3.2 Portable Electronic Device and Media Security

1. EPHI that is placed on portable electronic devices and media shall be encrypted so that access to the EPHI can only be attained by authorized individuals with knowledge of the decryption code.
2. Workforce members shall limit the quantity of EPHI on portable electronic devices and media to the minimum necessary for the performance of their duties.
3. Lockable devices shall be secured with a minimum 4 character password when not in use.
4. Devices with timeout capability shall utilize an inactivity timeout of no more than 15 minutes that require the user to enter their secure password to unlock the device.

5. All workforce members shall receive permission from their supervisor before transporting EPHI outside of the secured physical perimeter of a County facility. Approvals shall include the time period for authorization, which shall be a maximum of one year.
6. Workforce members shall not leave portable device or media that contains EPHI visible in their vehicles or in any other unsecured location.
7. Any EPHI on portable media or devices shall be saved on the network prior to movement or disposal.
8. DHHS workforce members who utilize USB devices shall purchase the device through Department of Technology (DTech) procurement. All others who use USB devices to store PHI will purchase encryptable devices and encrypt any folders containing PHI.
9. If portable media is lost, workforce members shall be responsible to immediately notify their supervisor.
10. Devices with the capability shall be remotely erased of EPHI data if lost, stolen or no longer used for County business.

7.3.3 Electronic Device and Media Disposal

Before electronic media that contains EPHI can be disposed, the following actions shall be taken on devices used by the workforce:

1. Hard drives shall be either wiped clean by IT or destroyed to prevent recognition or reconstruction of the information. The hard drive shall be tested to ensure the information cannot be retrieved.
2. Storage media, such as backup tapes, USB flash drives and CDs, shall be physically destroyed before disposing of the item to prevent recognition or reconstruction of the information.

7.3.4 Electronic Device and Media Reuse

All EPHI shall be removed from hard drives when the equipment is transferred to a worker who does not require access to the EPHI. Hard drives shall be wiped clean by DTech before transfer.

All other media shall have all the EPHI removed (the mechanism may vary depending on the media type) and tested to ensure the EPHI cannot be retrieved. If the media is not “technology capable” of being cleaned, the media shall be overwritten or destroyed.

7.3.5 Device Maintenance and Repair

When the technology is capable, all EPHI shall be removed from the device’s memory or hard drive before the device is accessed for maintenance or sent out for repair. Devices include computer servers, copiers, printers and other devices capable of storing electronic data.

7.3.6 Device and Media Acquisition

The County shall include security requirements and/or security specifications in information system acquisition contracts based on an assessment of risk (applications, servers, copiers, etc.).

7.4 Policy Responsibilities:

7.4.1 Manager and Supervisor Responsibilities

1. Ensure that only workforce members whose duties require the need to transport EPHI outside of the secured physical perimeter of a County facility are granted permission to do so.
2. Enforce procedures to govern the receipt and removal of hardware and electronic media that contain EPHI outside of the secured physical perimeter of a County facility, and the movement of these items within the facility.
3. Review this policy with workforce to ensure understanding of responsibilities regarding device and media controls.

7.4.2 DTech Support Responsibilities

1. Ensure all hard drives are wiped clean of EPHI before disposal, reuse or sent out for repair.
2. Maintain an inventory and a record of movements of hardware and electronic media such as workstation computers, servers, or backup tapes.

7.4.3 Workforce Member Responsibilities

1. Save an exact copy of EPHI on the network prior to movement or disposal of portable media and devices.
2. Follow the procedures that govern the receipt and removal of hardware and electronic media that contain EPHI.
3. Limit the quantity of EPHI on portable electronic media to the minimum necessary to perform their duties.
4. Secure EPHI on portable electronic media through encryption.
5. Remove and destroy all EPHI from portable electronic media when it is no longer needed to perform their duties.
6. Do not leave or store portable media that contains EPHI in their vehicles or in any other unsecured location.

(This page is intentionally blank)

Policy 8: Audit Controls

Issue Date: February 2005
Effective Date: April 21, 2005
Revised Date: February 29, 2016

8.1 HIPAA Regulation:

- *Log-in monitoring*
- *Information system activity review*
- *Audit controls*

8.2 Policy Purpose:

The purpose of this policy is to establish the standard of authority to conduct security monitoring and enforce audit controls on computing resources used by HIPAA covered components.

8.3 Policy Description:

The County has the requirement to monitor system access and activity of all HIPAA covered component workforce members.

8.3.1 Log-in Monitoring

To ensure that access to servers, workstations, and other computer systems containing electronic protected health information (EPHI) is appropriately secured, the following log-in monitoring measures shall be implemented:

1. A mechanism to record all failed log-in attempts on network systems containing EPHI when the technology is capable.
2. To the extent that technology allows, a means to disable any User ID that has more than four consecutive failed log-in attempts within a 30 minute period.
3. A review of log-in activity reports and logs when required to identify any patterns of suspicious activity, such as continuous failed log-in attempts.

8.3.2 Information System Activity Review

Information system activity reviews and audits may be conducted to:

1. Ensure integrity, confidentiality, and availability of information and resources.
2. Investigate possible security incidents to ensure compliance with County of Sacramento Department of Technology (DTech) and security policies.
3. Monitor user or system activity as required.
4. Verify that software patching is maintained at the appropriate security level.
5. Verify virus protection is current.

8.3.3 Information System Audit Controls

To ensure that activity for all computer systems accessing EPHI is appropriately monitored and reviewed, these requirements shall be met:

1. Where technology allows, the audit record shall capture sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.
2. Each fiscal quarter, at a minimum, DTech support shall review audit logs, activity reports, or other mechanisms for indications of improper use.
3. Indications of improper use shall be reported to management for investigation and follow up.
4. Audit logs of access to networks and applications with EPHI shall be archived and protected from unauthorized access, modification, and deletion.

8.4 Policy Responsibilities:

8.4.1 DTech Support Responsibilities

1. Implement and manage the log-in monitoring and audit controls through activity reports on systems containing EPHI to comply with the HIPAA Security Rule.
2. Report all suspicious log-in or system activity to management for investigation and follow-up.

8.4.2 Supervisor and Manager Responsibilities

1. Work with DTech support to ensure user and system activity reports provide sufficient information to determine if improper use of EPHI has occurred.
2. Work with DTech support to investigate reports of potential misuse of log-in accounts or access to EPHI by their workforce.

Policy 9: Security Incident Reporting and Response

Issue Date: February 2005
Effective Date: April 21, 2005
Revised Date: February 29, 2016

9.1 HIPAA Regulation:

- *Security incident procedures*
- *Reporting and response*

9.2 Policy Purpose:

The purpose of this policy is to formalize the response to, and reporting of, security incidents. This includes identification and response to suspected or known security incidents, the mitigation of the harmful effects of known or suspected security incidents to the extent possible, and the documentation of security incidents and their outcomes.

9.3 Policy Description:

The County shall identify, document, and respond to unauthorized use of the systems that contain electronic protected health information (EPHI).

9.3.1 Incident Reporting

Any intentional or unintentional, suspected or actual incident or event that affects, threatens, or violates the confidentiality, integrity or availability of electronic protected health information (EPHI) shall be reported immediately and responded to promptly.

Incidents that shall be reported include, but are not limited to:

1. Misdirected fax, email, print job or hard copy mail
2. Unencrypted email containing PHI that is sent outside the County network, or sent to the wrong person
3. Lost, stolen or missing laptop, smartphone, tablet, notebook, CD, USB or other portable device containing EPHI
4. Unauthorized alternation (change) deletion or corruption of PHI
5. EPHI data loss due to disaster, failure, error, theft
6. Loss of any electronic media that contains EPHI
7. Loss of the integrity of EPHI
8. Virus, worm, or other malicious code attacks
9. Persistent network or system intrusion attempts from a particular entity
10. Unauthorized access to EPHI, an EPHI based system or network
11. Facility incidents, including but not limited to:
    - Unauthorized person found in a HIPAA covered component's facility

- Facility break-in
- Lost, stolen, missing or misplaced key, C-Cure badge or cardkey

Workforce members shall notify their manager or supervisor of any suspected or confirmed security incident. The manager or supervisor shall report the incident to the Office of Compliance and the Department of Technology (DTech). Incidents may be reported directly to the Office of Compliance or the DTech Service Desk if the manager or supervisor is not available.

If a facility incident occurs, the manager or supervisor shall immediately report the incident to their facility manager, and to the IT Service Desk if appropriate.

If the security involves any breach of EPHI, the manager or supervisor shall notify the department's HIPAA Deputy Compliance Officer, in addition to notifying the Office of Compliance and the DTech Service Desk.

9.3.2 Incident Response and Resolution

The DTech Service Desk shall receive and record basic information on the incident and forward the information to the appropriate staff for response to that type of incident, i.e. a computer virus incident to the DTech staff that provides anti-virus support.

The Service Desk staff receiving the security incident service request shall perform their assigned responsibilities to respond to and/or mitigate any incident consequences. The DTech staff responsible for determining if a possible EPHI breach has resulted from the incident shall notify the Office of Compliance and the HIPAA Deputy Compliance Officer for the HIPAA covered component in which the incident occurred.

The Office of Compliance shall evaluate the incident to determine if a breach of EPHI occurred. If it is determined that a breach has occurred, the Office of Compliance, directed by the County Compliance Officer, shall contact County Counsel, law enforcement, Human Resources, or the County Communication and Media Office when it is deemed necessary.

The Office of Compliance shall coordinate any mandated notification process due to a confirmed breach of EPHI with the HIPAA Privacy Officer and HIPAA Security Officer, as applicable.

9.3.3 Incident Logging

All HIPAA security related incidents received by the Service Desk will be logged by the DTech Service Desk and documented by the assigned DTech support staff. The Office of Compliance shall document and log incidents and outcomes that are reviewed and investigated by the Office.

The Office of Compliance retains incident documentation a minimum of seven years.

9.4 Policy Responsibilities:

9.4.1 Workforce Member Responsibilities

Workforce members are responsible to promptly report any potential HIPAA incident to their manager or supervisor. Incidents may be reported directly to the Office of

Compliance if the manager or supervisor is not available, or directly to the DTech Service Desk.

9.4.2 Supervisor and Manager Responsibilities

1. Notify the DTech Service Desk at 874-5555 or online http://inside.dtech.saccounty.net/Pages/CreateIncident.aspx, or the Office of Compliance directly of any security incident.
2. Notify the facility manager of any facility related incident as described in Section 9.3.1.7.
3. Cooperate with incident documentation and investigation.
4. Mitigate as directed by Office of Compliance and government agencies as applicable.
5. Notify clients, applicable government agencies, and major media of breach, when applicable.

9.4.3 Facility Manager Responsibilities

Ensure that facility-related security incidents are reported and responded to as directed by the HIPAA covered component's policies and procedures.

9.4.4 DTech Service Desk Responsibilities

1. Log all reported security incidents for HIPAA covered components.
2. Notify DTech support teams as required by the incident type.

9.4.5 DTech Support Team Responsibilities

1. Perform their assigned duties to investigate, respond to, and/or mitigate any incident consequences.
2. Notify the Office of Compliance when a breach of EPHI is suspected or may have occurred.

9.4.6 Office of Compliance, HIPAA Deputy Compliance Officer (DCO), HIPAA Security Officer and HIPAA Privacy Officer Responsibilities

1. The Office of Compliance is responsible to determine if the incident requires further investigation and if it is a breach of EPHI. Working with the affected department's HIPAA DCO, the HIPAA Security Officer, and the HIPAA Privacy Officer, the Office of Compliance shall determine if corrective actions should be implemented.
2. If it is determined that a breach has occurred, the Office of Compliance, directed by the County Compliance Officer, shall contact County Counsel, law enforcement, Human Resources, or the County Communication and Media Office when it is deemed necessary.
3. The Office of Compliance is responsible for documentation of EPHI breach investigations and any corrective actions.
4. The Office of Compliance is responsible for maintaining all documentation on EPHI breaches for a minimum of 7 years.

5. The Office of Compliance is responsible for breach reporting to the federal Department of Health and Human Services or applicable agency.
6. The Office of Compliance shall coordinate any mandated notification process due to a confirmed breach of EPHI with the HIPAA Privacy Officer and HIPAA Security Officer.

Policy 10: Transmission Security

Issue Date: February 2005
Effective Date: April 21, 2005
Revised Date: February 29, 2016

10.1 HIPAA Regulation:

- *Transmission security*
- *Integrity controls*
- *Encryption*

10.2 Policy Purpose:

The purpose of this policy is to guard against unauthorized access to, or modification of, electronic protected health information (EPHI) that is being transmitted over an electronic communications network. When EPHI is transmitted from one point to another, it shall be protected in a manner commensurate with the associated risk.

10.3 Policy Description:

10.3.1 Encryption

Whenever possible, Advanced Encryption Standard (AES) for the encryption algorithm should be used for its strength and speed. The use of proprietary encryption algorithms is not allowed for any purpose unless authorized by the Chief Information Security Officer (CISO).

10.3.1.1 Encryption Required

1. No EPHI shall be sent outside the County of Sacramento Wide Area Network (CoSWAN) unless it is encrypted. This includes all email and email attachments sent over the Internet.
2. When accessing a secure network an encryption communication method, such as Virtual Private Network (VPN), shall be used.

10.3.1.2 Encryption Optional

1. When using a private circuit (point to point) to transmit EPHI, such as authorized transmission of EPHI within the CoSWAN, no encryption is required.
2. Dialup connections directly into secure networks are considered to be secure connections for EPHI and no encryption is required.

10.3.2 Transmission and Modem Use

1. Dialing directly into or out of a workstation in a HIPAA covered component that is simultaneously connected to a Local Area Network (LAN), the CoSWAN, or another internal communication network is prohibited.
2. Modems shall never be left connected to workstations in HIPAA covered components.

10.3.3 EPHI Transmissions Using Wireless Networks

1. The transmission of EPHI over a wireless network is permitted if both of the following conditions are met:
    a. The connection through the wireless network utilizes an authentication mechanism to ensure that wireless devices connecting to the network are authorized; and
    b. The connection through the wireless network utilizes an encryption mechanism for all transmissions over the network.
2. If transmitting EPHI over a wireless network that is not utilizing an authentication and encryption mechanism, the EPHI shall be encrypted before transmission.
3. Wireless devices are not to be connected to a wireless access point and to the CoSWAN at the same time. Wireless access capability must be disabled on any device that is connected to the CoSWAN.

10.3.4 Perimeter Security

1. Any external connection to the CoSWAN shall come through the perimeter security's managed point of entry.
2. If determined safe by the Perimeter Security Team, outbound services shall be initiated for internal addresses to external addresses.
3. Inbound services shall be negotiated on a case by case basis with the Perimeter Security Team.
4. All workforce members connecting to the CoSWAN shall sign the Sacramento County IT Security Policy before connectivity is established.

10.3.5 Firewall Controls

1. Networks containing systems and applications with EPHI shall implement perimeter security and access control with a firewall.
2. Firewalls shall be configured to support the following minimum requirements:
    a. Limit network access to only authorized workforce members and entities
    b. Limit network access to only legitimate or established connections
    c. Console and other management ports shall be appropriately secured or disabled
3. The configuration of firewalls used to protect networks containing EPHI based systems and applications shall be submitted to the Perimeter Security Team for review and approval.

10.4 Policy Responsibilities:

10.4.1 Workforce Member Responsibilities

All workforce members that transmit EPHI outside the CoSWAN are responsible for ensuring the information is safeguarded by using encryption when using the Internet or a wireless connection.

10.4.2 Department of Technology Support Responsibilities

The County of Sacramento Perimeter Security Team is responsible for the perimeter security architecture, its resources, its periodic auditing, and testing.

(This page is intentionally blank)

Policy 11: Protection from Malicious Software

Issue Date: February 2005
Effective Date: April 21, 2005
Revised Date: January xx, 2016

11.1 HIPAA Regulation:

- *Protection from malicious software*

11.2 Policy Purpose:

The purpose of this policy is to establish criteria for protections to guard against, detect, and report malicious software. Malicious software includes, but is not limited to, viruses, worms, malware and spyware.

11.3 Policy Description:

The County of Sacramento shall implement and maintain current anti-virus software on all servers and workstations (owned, leased, and/or operated by the HIPAA covered components). All workstations shall be configured to activate and update anti-virus software automatically whenever the computer is turned on and connected to the network.

In the event that a virus, worm, or other malicious code has infected or been identified on a server or workstation that poses a significant risk, that equipment shall be disconnected from the network until it has been appropriately cleaned.

11.4 Responsibilities:

11.4.1 Workforce Member Responsibilities

1. Disabling automatic virus scanning features is prohibited.
2. Maintain current anti-virus software on their non-County computer that is used to access EPHI.
3. Immediately contact the manager or supervisor and the IT Service Desk if a virus is suspected, as explained in **Section 9.3.1 Incident Reporting**.

11.4.2 Department of Technology (DTech) Support Responsibilities

1. Computers that connect to the County of Sacramento Wide Area Network (CoSWAN) shall be equipped with anti-virus software before allowing such computers to connect to the CoSWAN. The Chief Information Officer (CIO) may deny access to computers that do not have updated anti-virus software installed.
2. Configure laptops to activate and update anti-virus software automatically whenever the computer is turned on and connected to the network.
3. Inform HIPAA covered component management of any new virus, worm, or other type of malicious code that may be a threat to EPHI.

4. Disconnect any server or workstation from the County network until it has been appropriately cleaned if infected by a virus, worm or other malicious code that poses a threat to EPHI.
5. Maintain a log of virus infections and detections that includes a record of successful eradication of viruses and cleaning of affected files and computer applications.
6. Maintain network based security hardware and software to protect against viruses, hacking and unauthorized access.
7. Maintain antivirus security patches and updates.
8. Follow Federal Risk and Authorization Management Program (FedRAMP) standards for security of high-risk non-County hosted cloud system.

11.4.3 Manager and Supervisor Responsibilities

1. Ensure that laptops used to logon to the network shall have all anti-virus software updates installed by DTech support.
2. Ensure workforce members are made aware of the threats and vulnerabilities due to malicious code and software such as viruses and worms.
3. Inform workforce members of any of new virus, worm, or other type of malicious code that may be a threat to EPHI.

Policy 12: Contingency Plan

Issue Date: February 2005
Effective Date: April 21, 2005
Revised Date: February 29, 2016

12.1 HIPAA Regulation:

- *Contingency plan*
- *Data backup plan*
- *Disaster recovery plan*
- *Emergency mode operation plan*
- *Testing and revision procedures*
- *Applications and data criticality analysis*
- *Contingency operations*

12.2 Policy Purpose:

The purpose of this policy is to establish rules to protect the availability, integrity and security of electronic protected health information (EPHI) from the impact of natural, human, and environmental risks while continuing business while continuing business without the normal resources of the organization.

12.3 Policy Description:

Each HIPAA covered component shall have documented procedures for implementation in the event of an emergency, disaster or other occurrence (i.e., fire, vandalism, system failure and natural disaster) when any system that contains EPHI is affected, including:

- Applications and Data Criticality Analysis
- Data Backup Plan
- Disaster Recovery Plan
- Emergency Mode Operation Plan

Each of the following plans shall be evaluated and periodically updated as business needs and technology requirements change.

12.3.1 Applications and Data Criticality Analysis

1. Each HIPAA covered component shall periodically assess the relative criticality of applications and data used by the HIPAA covered component for purposes of maintaining a current Data Backup Plan, Disaster Recovery Plan and Emergency Mode Operation Plan.
2. Each HIPAA covered component shall identify critical business functions, define impact scenarios, and determine resources needed to recover from each impact.

12.3.2 Data Backup Plan

1. All EPHI shall be stored on network servers in order for it to be automatically backed up by the system.
2. EPHI shall not be saved on the local (C:) drive of any workstation.
3. EPHI stored on portable media shall be saved to the network to ensure backup of the EPHI.
4. Department of Technology (DTech) support shall establish and implement a Data Backup Plan that, at a minimum, includes daily backups of user-level and system-level information and weekly backups that are stored securely offsite.
5. The Data Backup Plan shall apply to all files that may contain EPHI.
6. The Data Backup Plan shall require that all media used for backing up EPHI be stored in a physically secure environment.
7. Data backup procedures outlined in the Data Backup Plan shall be tested on at least an annual basis to ensure that exact copies of EPHI can be retrieved and made available.

12.3.3 Disaster Recovery Plan

1. To ensure that HIPAA covered components can recover from the loss of data due to an emergency or disaster such as fire, vandalism, system failure, or natural disaster affecting systems containing EPHI, DTech support shall establish and implement a Disaster Recovery Plan for restoring or recovering loss of EPHI and the systems needed to make that EPHI available in a timely manner.
2. The Disaster Recovery Plan shall be documented and be available to the assigned personnel, who shall be trained to implement the Disaster Recovery Plan.
3. The disaster recovery procedures outlined in the Disaster Recovery Plan shall be tested on a periodic basis to ensure that EPHI and the systems needed to make EPHI available can be restored or recovered.

12.3.4 Emergency Mode Operation Plan

1. Each HIPAA covered component shall document and implement procedures to enable continuation of critical business processes for the protection of EPHI while operating in emergency mode. Emergency mode operation must include processes to protect the security of EPHI during and immediately after a crisis.
2. Emergency mode operation procedures outlined in the Emergency Mode Operation Plan shall be tested periodically.

12.4 Policy Responsibilities:

12.4.1 Manager and Supervisor Responsibilities

1. Develop and document an Emergency Operations Mode Plan for their units that include appropriate procedures for their workforce.

2. Annually ensure that appropriate emergency operations and disaster recovery procedures are in place.
3. Periodically test their Emergency Operations Mode Plan.
4. Ensure that workforce members save all EPHI on network drives and not on the local drive (C:) of their workstation.

12.4.2 DTech Support Responsibilities

1. Establish, implement and document the Data Backup Plan for EPHI used in the HIPAA covered components.
2. Annually test the EPHI backups to ensure that exact copies of EPHI can be retrieved.
3. Document and maintain a Disaster Recovery Plan to restore the EPHI applications and data that is needed for the HIPAA covered components to continue their critical business functions in a disaster.
4. Periodically test the documented disaster recovery procedures to ensure EPHI data and systems can be restored.

(This page left intentionally blank)

Policy 13: Business Associate Contracts

Issue Date: February 2005
Effective Date: April 21, 2005
Revised Date: February 29, 2016

13.1 HIPAA Regulation:

- *Business associate contracts and other arrangements*
- *Written contract or other arrangements*

13.2 Policy Purpose:

The purpose of this policy is to document the process for determining, documenting and monitoring those contractual and business relationships that are considered "Business Associates" as defined by the HIPAA Security Rule.

13.3 Policy Description:

13.3.1 Business Associate Determination

In order to determine if a contractual or business relationship entered into by a HIPAA covered component of the County of Sacramento meets the definition of a HIPAA Business Associate as defined by legal mandate, the following process shall be followed:

1. When a contract is developed and managed by the Contract Division of a HIPAA covered component, it shall ensure that a HIPAA Business Associate Decision Tool (HIPAA Form 3011) is completed to determine if a Business Associate agreement is required.
2. When a contract is developed and managed by the Department of General Services, Contracts and Purchasing Division, the designated Contract Services Officer shall coordinate with the HIPAA covered component user(s) to determine if the contract meets the definition of a Business Associate. This coordination shall include ensuring the HIPAA Form 3011 is completed.
3. Every HIPAA Form 3011 shall be provided to County Counsel for review and final determination of possible Business Associate status before the contract is signed.
4. If a Business Associate agreement is required, the HIPAA covered component's Contract Division or the designated General Services Contract Services Officer shall ensure an exhibit approved by County Counsel is included in the contract.

13.3.2 Business Associate Tracking

The Office of Compliance shall maintain a database of all County Business Associates. This information shall be provided to the Office of Compliance in a semi-annual report by the General Services Contract and Purchasing Division and by the Contract Divisions of the HIPAA covered components.

The Contract Divisions of the HIPAA covered components shall provide the Office of Compliance semi-annual notification of all other arrangements, (e.g. Memorandums of Understanding (MOUs) with HIPAA Business Associates that are governmental entities).

13.3.3 Business Associate Monitoring

If the County knows of a pattern of activity or practice that constitutes a material breach or violation of an obligation of the Business Associate under the contract or other arrangement, the County shall take reasonable steps to repair the breach or end the violation, as applicable.

This shall include working with, and providing consultation to, the Business Associate. If such steps are unsuccessful, County of Sacramento shall terminate the contract or arrangement, if feasible. If termination is not feasible, the problem shall be reported to the Secretary of the federal Department of Health and Human Services, Office for Civil Rights (OCR).

County Counsel, the HIPAA covered component's HIPAA Deputy Compliance Officer, the County Compliance Officer and the HIPAA Security Officer shall be informed of any incident of non-compliance with HIPAA Business Associate provisions. Documentation of any incident of non-compliance, and outcomes of the subsequent investigation, shall be provided to the Office of Compliance by the HIPAA covered component.

13.4 Policy Responsibilities:

13.4.1 Workforce Member Responsibilities

Immediately provide information regarding any complaint or report from any source about inappropriate safeguards to electronic protected health information (EPHI) by Business Associate contractors to their manager or supervisor.

13.4.2 Manager and Supervisor Responsibilities

1. Respond to any pattern of activity or practice of a HIPAA Business Associate that constitutes a material breach or violation of an obligation of the Business Associate, under the contract or other arrangement, by documenting the incident.
2. Promptly inform and work with County Counsel, the HIPAA covered component's HIPAA Deputy Compliance Officer, and the County Compliance Officer to repair the breach, end the violation, and/or terminate the contract, as applicable.

13.4.3 Contract Managers - HIPAA Covered Components

1. Coordinate with user(s) to assess whether contracts meet the definition of a Business Associate and ensure the HIPAA Form 3011 is completed.
2. Ensure the completed HIPAA Form 3011 is provided to County Counsel for review and final determination before the contract is signed.
3. Provide the Office of Compliance with semi-annual notification of all Business Associate agreements, including other arrangements such as MOUs with governmental entities that are Business Associates, managed by the HIPAA covered component.

13.4.4 General Services Contract and Purchasing Division

1. Ensure that designated Contract Services Officers coordinate with the HIPAA covered component user(s) to assess whether the contracts meet the definition of a Business Associate, and the HIPAA Form 3011 is completed.
2. Provide the HIPAA Form 3011 to County Counsel for review and final determination before the contract is signed.
3. Provide the Office of Compliance with semi-annual notification of all Business Associate agreements managed by the General Services Contract and Purchasing Division.

13.4.5 Office of Compliance Responsibilities

1. Maintain a database of all County HIPAA Business Associates managed by the General Services Contract and Purchasing Division and by the Contract Divisions of the HIPAA covered components.
2. Coordinate, as assigned by the County Compliance Officer or the HIPAA Security Officer, with the HIPAA covered components in responding to a report of any pattern of activity or practice that constitutes a material breach or violation of an obligation of a Business Associate.

13.4.6 County Counsel Responsibilities

Provide review of HIPAA Forms 3011 for final determination of Business Associate status before a contract is signed.

(This page left intentionally blank)

Policy 14: Risk Analysis and Management

Issue Date: February 2005
Effective Date: April 21, 2005
Revised Date: February 29, 2016

14.1 HIPAA Regulation:

- *Perform a periodic technical and non-technical evaluation*
- *Security management process*
- *Risk analysis*
- *Risk management*

14.2 Policy Purpose:

The purpose of this policy is to establish periodic evaluations of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (EPHI) held by the County's HIPAA covered components and to manage the security of the EPHI by identifying, controlling and mitigating risks.

14.3 Policy Description:

The County's HIPAA covered components with the Office of Compliance shall perform risk analysis and management through periodic assessments and implementation of controls to mitigate risks.

14.3.1 Risk Analysis

In order to conduct an accurate and thorough assessment of potential risks and vulnerabilities to the EPHI held by the County's HIPAA covered components, the following activities shall be conducted and documented by the Office of Compliance:

1. Periodic program assessments including a security review of facility access controls, protection of network server closets, workstations, portable devices, and document destruction capabilities.
2. Assessments of new or existing information system applications that contain, or are used to protect, EPHI.
3. Assessments of modifications to existing facilities or development of new facilities that maintain or house EPHI.
4. Assessments of new programs, departments or changes in the mode or manner of service delivery involving EPHI.

14.3.2 Risk Management

Security measures and controls, sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level, shall be implemented:

1. Workforce security training and awareness reminders
2. Access controls, authorization and validation procedures

3. Detection and activity reviews
4. Applications and data criticality analysis
5. IT systems change management
6. Incident reporting and response procedures
7. Sanctions for noncompliance
8. Contingency, Data Backup and Disaster Recovery Planning

14.3.2.1 Department of Technology (DTech) Change Management

The risk management process shall include change controls for all alterations that occur in the information systems that support, contain, or protect EPHI. These alterations include, but are not limited to:

1. Installation, update or removal of network services and components
2. Operating systems upgrades
3. Installation, update or removal of applications, software and database servers.

DTech change management notification and implementation shall follow the policies and procedures as documented by DTech support.

14.4 Policy Responsibilities:

14.4.1 DTech Support Responsibilities

1. Inform the Office of Compliance of the planned installation, update or removal of any applications containing EPHI in a HIPAA covered component.
2. Follow approved County IT Change Management Policies and Procedures (http://inside.dtech.saccounty.net/StaffResources/ChangeManagement/Pages/default.aspx) for all alterations that occur in the information systems that support, contain, or protect EPHI.
3. DTech Support shall assist the Office of Compliance with risk analysis activities as needed.

14.4.2 Office of Compliance Responsibilities

Office of Compliance is responsible for risk analysis activities as indicated in **Section 14.3.1**

Policy 15: Security Awareness and Training

Issue Date: February 2005
Effective Date: April 21, 2005
Revised Date: February 29, 2016

15.1 HIPAA Regulation:

- *Security awareness and training*
- *Security reminders*

15.2 Policy Purpose:

The purpose of this policy is to ensure that the County's workforce in the HIPAA covered components receive the necessary training to comply with the County HIPAA Security Policies and Procedures and prevent any violations of confidentiality, integrity or availability of electronic protected health information (EPHI).

15.3 Policy Description:

Workforce training is required to protect EPHI held by the County's HIPAA covered components.

15.4 Training Standards

15.4.1 Systems and Applications

Each HIPAA covered component shall train their workforce, at a minimum, on the following security standards for all systems and applications where access has been granted:

1. Proper uses and disclosures of the EPHI stored in the application.
2. How to properly log on and log off the application containing EPHI.
3. Instructions on contacting a manager or supervisor or Department of Technology (DTech) Service Desk when EPHI may have been altered or destroyed due to user error.
4. Instructions on reporting a potential security breach to a supervisor, manager or directly to the Office of Compliance or DTech Service Desk.
5. Instructions regarding internet security, virus protection, password security and confidential data handling.

15.4.2 County HIPAA Security Policies and Procedures

The Office of Compliance will provide HIPAA security training to all workforce members of the County's HIPAA covered components on the County's HIPAA Security Policies and Procedures, and shall maintain training records for a period of at least six years.

The training will be specific to the roles and responsibilities of the workforce at the worker level and the manager or supervisor level.

All new workforce members in HIPAA covered components are required to attend the appropriate training within 60 days of assuming their position. Workforce members shall attend retraining at a minimum of every 3 years or at a frequency determined by the County Compliance/HIPAA Privacy Officer.

Each HIPAA covered component is required to ensure all of their workforce members receive training.

15.4.3 HIPAA Security Reminders

The Office of Compliance, in coordination with the HIPAA covered components and the HIPAA Deputy Compliance Officers, shall develop and issue periodic reminders on security awareness to the County's HIPAA covered workforce using any media that is most effective for each HIPAA covered component (e.g. email, posters, newsletters, intranet site, etc).

15.5 Policy Responsibilities:

15.5.1 Manager and Supervisor Responsibilities

1. Ensure that all HIPAA workforce members in their operational areas are trained on the systems and application security listed in **Section 15.4.1** of this policy.
2. Ensure that all workforce members in their operational areas are enrolled in one of the training classes provided by the Office of Compliance within 60 days of the workforce member assuming their position in the HIPAA covered component, and thereafter once every three years or at a frequency determined by the County Compliance/HIPAA Privacy Officer.

15.5.2 Workforce Member Responsibilities

1. Workforce members in HIPAA covered components shall complete HIPAA training within 60 days of assuming their position, and thereafter once every three years or at a frequency determined by the County Compliance/HIPAA Privacy Officer; shall sign the HIPAA Privacy and Security Practices Acknowledgment Form 3012; and provide the signed form to their supervisor or to the Office of Compliance.
2. Temporary agency workforce members, volunteers, and contracted workers that access EPHI are required to complete HIPAA training as required by the Office of Compliance and shall provide the Office of Compliance a signed copy of the HIPAA Privacy and Security Practices Acknowledgment Form 3012.

15.5.3 Office of Compliance Responsibilities

1. The Office of Compliance has oversight responsibility to audit reports to ensure required workforce member attendance. As directed by the County Compliance/HIPAA Privacy Officer and the HIPAA Security Officer, the Office of Compliance may require workforce members to attend more training if security incidents warrant this remedial action.

2. The Office of Compliance or its designee shall provide HIPAA security training, track completion of the training in COMPASS, and maintain training records for a minimum of six years.
3. The Office of Compliance, in coordination with the HIPAA covered components and the HIPAA Deputy Compliance Officers, shall provide periodic security reminders to HIPAA covered component workforce.

(This page is intentionally blank)

Policy 16: Sanctions

Issue Date: February 2005
Effective Date: April 21, 2005
Revised Date: February 29, 2016

16.1 HIPAA Regulation:

- *Sanction policy*

16.2 Policy Purpose:

The purpose of this policy is to ensure that workforce members of the County's HIPAA covered components are informed of sanctions, penalties and disciplinary actions that may be applied for non-compliance with the County's HIPAA Security Policies and Procedures.

16.3 Policy Description:

Workforce members are accountable for their actions in failing to comply with HIPAA Security Rule requirements, as defined in the County's HIPAA Security Policies and Procedures.

16.3.1 Sanctions

Members of the County of Sacramento HIPAA covered component workforce who violate County of Sacramento HIPAA Security Policies and Procedures regarding the safeguarding of electronic protected health information (EPHI) are subject to disciplinary action by County of Sacramento up to and including immediate dismissal from employment or service. For violations of these polices, corrective action, including but not limited to contract cancellation or termination of services, shall be implemented by the County for those members of the workforce who are not subject to the County discipline process.

Members of the County of Sacramento HIPAA covered component workforce who knowingly and willfully violate state or federal law for failure to safeguard EPHI are subject to criminal investigation, prosecution and/or civil monetary penalties.

If the County of Sacramento fails to enforce security safeguards, the County may be subject to administrative penalties by the federal Department of Health and Human Services Office for Civil Rights, including federal funding penalties; and/or fines and penalties by the California Office of Health Information and Integrity.

16.3.2 Reporting Violations

All workforce members shall notify their manager or supervisor, the Office of Compliance, or their HIPAA Deputy Compliance Officer when there is a reasonable belief that any security policies or procedures are being violated.

16.3.3 Retaliation Prohibited

Neither the County of Sacramento as an entity nor any member of the County of Sacramento HIPAA covered workforce shall intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against any individual for:

1. Exercising any right established under the County's HIPAA Security Policies and Procedures
2. Participating in any process established by County HIPAA Security policy, including the filing of a complaint with the County of Sacramento or with the federal Department of Health and Human Services Office for Civil Rights
3. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing relating to the County's policies and procedures
4. Opposing any unlawful act or practice, provided that the individual or other person (including a member of the County of Sacramento workforce) has a good faith belief that the act or practice being opposed is unlawful and the manner of such opposition is reasonable and does not involve a use or disclosure of an individual's protected confidential information in violation of County of Sacramento policy.

Any workforce member who engages in retaliation shall be subject to the sanctions under this policy.

16.4 Policy Responsibilities:

16.4.1 Workforce Member Responsibilities

1. All HIPAA covered component workforce members shall comply with the County HIPAA Security Policies and Procedures.
2. All HIPAA covered component workforce members shall notify their manager or supervisor or the HIPAA Deputy Compliance Officer of their department or division if they have a reasonable belief that any security policies or procedures are being violated.
3. All HIPAA covered component workforce members are required to sign HIPAA Acknowledgement Form 3013, certifying they have received training on the Countywide HIPAA Privacy and Security Policies and Procedures, and will comply with the Countywide HIPAA Privacy and Security Policies and Procedures.

Appendix A - HIPAA Security Rule / County Policies Crosswalk

HIPAA Security Rule	Section	Policy #
Security Management Process	164.308(a)(1)	14
Risk Analysis		14
Risk Management		14
Sanction Policy		16
Information System Activity Review		8
Assigned Security Responsibility	164.308(a)(2)	1
Workforce Security	164.308(a)(3)	3
Authorization and/or Supervision		3
Workforce Clearance Procedure		3
Termination Procedures		3
Information Access Management	164.308(a)(4)	3
Access Authorization		3
Access Establishment and Modification		3
Security Awareness & Training	164.308(a)(5)	15
Security Reminders		15
Protection from Malicious Software		11
Log-in Monitoring		8
Password Management		4
Security Incident Procedures	164.308(a)(6)	9
Reporting and Response		9
Contingency Plan	164.308(a)(7)	12
Data Backup Plan		12
Disaster Recovery Plan		12
Emergency Mode Operation Plan		12
Testing and Revision Procedure		12
Applications and Data Criticality Analysis		12
Evaluation	164.308(a)(8)	14

Business Associate Contracts and Other Arrangements	164.308(b)(1)	13
Written Contract or Other Arrangements		13
Facility Access Controls	164.310(a)(1)	5
Contingency Operations		5
Facility Security Plan		5
Access Control and Validation Procedures		5
Maintenance Records		5
Workstation Use	164.310(b)	6
Workstation Security	164.310(c)	6
Device and Media Controls	164.310(d)(1)	7
Disposal		7
Media Re-use		7
Accountability		7
Data Backup and Storage		7
Access Control	164.312(a)(1)	3
Unique User Identification		4
Emergency Access Procedure		3
Automatic Logoff		6
Encryption and Decryption		10
Audit Controls	164.312(b)	8
Integrity	164.312(c)(1)	4
Mechanism to Authenticate Electronic Protected Health Information		4
Person or Entity Authentication	164.312(d)	4
Transmission Security	164.312(e)(1)	10
Integrity Controls		10
Encryption		10
Policies and Procedures	164.316(a)	2
Documentation	164.316(b)(1)	2
Notification in the Case of Breach	Subpart D, 164.400	9

Appendix B – Mapping County Policies to HIPAA Regulations

Policy 1: Assigned Security Responsibility

HIPAA Regulation Covered:

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.

Policy 2: Policy Documentation

HIPAA Regulation Covered:

Policies and procedures. Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, if the changes are documented and are implemented in accordance with this subpart.
Documentation. (i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.
Time limit. Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.
Availability. Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.
Updates. Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

Policy 3: User Access Management

HIPAA Regulation Covered:

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.
Authorization and/or supervision. 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.

Workforce clearance procedure. Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.
Termination procedures. 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.
Information access management. Establish and maintain formal, documented policies and procedures for authorizing access to EPHI consistent with the Privacy Rule. These policies should also define how access is granted and modified.
Access authorization. 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.
Access establishment and modification. 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."
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).
Integrity. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.
Emergency access procedure. Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

Policy 4: Authentication and Password Management

HIPAA Regulation Covered:

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

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

Password management. Procedures for creating, changing, and safeguarding passwords.
Unique user identification. Assign a unique name and/or number for identifying and tracking user identity.

Policy 5: Facility Access Controls

HIPAA Regulation Covered:

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

Access control and validation procedures. 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.
Maintenance records. 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).
Contingency operations. 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.

Policy 6: Workstation Security

HIPAA Regulation Covered:

Access control and validation. Implement procedures to control and validate a person's access to electronic protected health information based on their role or function.
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.
Workstation security. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized workforce members.
Automatic logoff. Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

Policy 7: Device and Media Controls

HIPAA Regulation Covered:

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.
Disposal. 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.
Media re-use. Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.
Accountability. Maintain a record of the movements of hardware and electronic media and any person responsible therefore.
Data backup and storage. Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

Policy 8: Audit Controls

HIPAA Regulation Covered:

Log-in monitoring. Procedures for monitoring log-in attempts and reporting discrepancies.

Information system activity review. Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
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.

Policy 9: Security Incident Reporting and Response

HIPAA Regulation Covered:

Security incident procedures. Implement policies and procedures to address security incidents.

Reporting and response. 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.

Notification in the event of breach. Implement policies and procedures to provide notification in the event of breaches of unsecured protected health information.

Policy 10: Transmission Security

HIPAA Regulation Covered:

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.

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

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

Policy 11: Protection from Malicious Software

HIPAA Regulation Covered:

Protection from malicious software. Procedures for guarding against, detecting, and reporting malicious software.

Policy 12: Contingency Plan

HIPAA Regulation Covered:

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

Disaster recovery plan. Establish (and implement as needed) procedures to restore any loss of data.
Emergency mode operation plan. 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.
Testing and revision procedures. Implement procedures for periodic testing and revision of contingency plans.
Applications and data criticality analysis. Assess the relative criticality of specific applications and data in support of other contingency plan components.
Contingency operations. 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.

Policy 13: Business Associate

HIPAA Regulation Covered:

Business associate contracts and other arrangements. A covered entity, in accordance with 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 that the business associate shall appropriately safeguard the information.
Written contract or other arrangements. A written contract or agreement that documents the satisfactory assurances of the business associate that it shall safeguard the EPHI shall be obtained between any covered entity and its business associates.

Policy 14: Risk Analysis and Management

HIPAA Regulation Covered:

Perform a periodic technical and non-technical evaluation, 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 this subpart".
Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations.
Risk analysis. 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.
Risk management. Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level

Policy 15: Security Awareness and Training

HIPAA Regulation Covered:

Security awareness and training. Implement a security awareness and training program for all members of its workforce (including management).
Security reminders. Periodic security updates.

Policy 16: Sanctions

HIPAA Regulation Covered:

Sanction policy. Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.

County of Sacramento HIPAA Security Rule
Policies and Procedures

~END~