County of El Dorado

Health Insurance Portability and Accountability Act (HIPAA)

Privacy and Security Policies and Procedures

II: HIPAA Security Rule

Issue Date: August 8, 2017

Effective Date: August 8, 2017

Introduction

Effective August 8, 2017, the County of El Dorado HIPAA Security Rule Policies and Procedures are revised in accordance with *Policy 2.3.1(a)* and *(b)*. Changes in business practices of the County's HIPAA covered components as well as changes in mandated federal law required this revision.

The HIPAA Security Rule Policies and Procedures can be accessed electronically at https://www.edcgov.us/government/bos/Policies/pages/Policy_Manual.aspx

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.
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, Human Resources-Risk Management, County Counsel, Procurement and Contracts, Information Technology, and Treasurer-Tax Collector, 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.
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, , CDs, optical devices, tablets, smartphones) **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; • The provision of health care to the individual; or • The past, present, or future payment for the provision of health care to the individual.

Terms	Definitions
	<u>Exceptions: PHI and/or EPHI does not include the following:</u> • Education records • Workers' 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 Electronic Protected Health Information (EPHI).
Firewalls	Special computer programs and hardware that are set up on a network 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 Information Technology Department
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	Malicious software, commonly known as malware, is any software that brings harm to a computer system. Malware can be in the form of worms, viruses, trojans, spyware, adware and rootkits, etc., which steal protected data, delete documents or add software not approved by a user.
Media reuse	A device such as a computer hard drive that contained data (information) that is being reused to contain new data.
Network	A group of computers (workstations) and associated devices connected by a communications channel to share information 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.

Terms	Definitions
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: CDs; USB drives (or memory sticks/flash drives, smartphones, and tablets.
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	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 eight 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.
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	Credentials issued for access privileges, which identifies the user

Terms	Definitions
	to County IT systems.
Virtual Private Network (VPN)	An encrypted network connection between two or more devices across the public internet or other shared network. It allows workstation computers at different locations to send encrypted communications to each other.
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." Workforce members include supervisors, managers and line staff.
Workstation	A laptop or desktop computer, or any other device that performs computer functions.

Policy 1: Assigned Security Responsibility

Issue Date: August 8, 2017
Effective Date: August 8, 2017
Revised Date: n/a

1.1 HIPAA Regulation:

- *Assigned security responsibility*

1.2 Policy Purpose:

At all times the County of El Dorado 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 El Dorado County in all issues related to HIPAA security.

1.4 Policy Responsibilities:

The above HIPAA Security Officer responsibilities are assigned to the Information Security Officer for the County of El Dorado, as appointed by the Director of Information Technologies.

The HIPAA Security Officer shall coordinate the program level support for the HIPAA Security Rule implementation with the County's Privacy Officer.

Policy 2: Policy Documentation

Issue Date: August 8, 2017
Effective Date: August 8, 2017
Revised Date: n/a

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 El Dorado HIPAA Security Rule Policies and Procedures are created and maintained in accordance with federal regulations.

2.3 Policy Description:

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

2.3.1 Policies and Procedures

1. The HIPAA Security Officer, the HIPAA Privacy Officer 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 HIPAA Privacy Officer and existing IT governance bodies shall participate in the revision process.
3. The County HIPAA Privacy Officer, shall direct 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 Information Security Officer who is assigned the responsibilities of the HIPAA Security Officer.
4. All policies and procedures implemented to comply with the HIPAA Security Rule shall be made available to the HIPAA covered component workforce.
5. 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.

6. 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.
7. 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 County Information Security Officer and HIPAA Security Officer

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.

2.4.2 County Compliance Officer and HIPAA Privacy Officer Responsibilities

Direct the HIPAA Privacy Officer 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 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: August 8, 2017
Effective Date: August 8, 2017
Revised Date: n/a

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, is under the direct control of such entity, whether or not they are paid by the covered entity."

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 El Dorado's General Network Usage Policy* before access is granted to the network or any application that contains EPHI, and thereafter shall comply with all County of El Dorado 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 El Dorado County General Network Usage Policy and the El Dorado 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.

Policy 4: Authentication and Password Management

Issue Date: August 8, 2017
Effective Date: August 8, 2017
Revised Date: n/a

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 EPHI.

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 90 days
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 El Dorado 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

Select strong passwords that have the following characteristics:

1. The password contains at least 8 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.

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 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.

4.4.3 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

Policy 5: Facility Access Controls

Issue Date: August 8, 2017
Effective Date: August 8, 2017
Revised Date: n/a

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 electronic protected health information (EPHI).

5.3 Policy Description:

The County of El Dorado shall reasonably safeguard electronic protected health information (EPHI) from any intentional or unintentional use or disclosure. The County shall protect its facilities where EPHI 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 County Privacy Officer shall periodically audit HIPAA covered component facilities to ensure EPHI safeguards are continuously being maintained.

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

The following shall be implemented for all sites that access EPHI:

1. **Visitor Access Control:** In facilities in which 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 EPHI is accessible.
2. **Security Access Cardkeys:** Some facilities 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). These facilities 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 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

3. **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.

4. **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.

5. **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.

6. **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.

7. **Alarm Systems:** All buildings that contain 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.

8. **Doors**: All non-public exterior doors (such as employee only doors) and doors leading to areas with 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.

5.3.3 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 EPHI as well as support restoration of lost 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.

5.3.4 Maintenance Records

Repairs or modifications to the physical building for each facility where 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.

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.
4. Immediately report lost or stolen cardkeys, metal keys or keypad-cipher lock combinations.
5. Surrender access cardkeys and/or hard key(s) upon leaving employment.

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. .
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 Privacy Officer

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.

Policy 6: Workstation Security

Issue Date: August 8, 2017
Effective Date: August 8, 2017
Revised Date: n/a

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). 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 El Dorado 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 using the Ctrl-Alt-Delete-Enter keys 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-use machines 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 IT 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: August 8, 2017
Effective Date: August 8, 2017
Revised Date: n/a

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.

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, , tablets, smartphones, 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 Media Security

EPHI that is placed on portable electronic media shall be encrypted so that access to the EPHI can only be attained by authorized individuals with knowledge of the decryption code.

Workforce members shall limit the quantity of EPHI on portable electronic media to the minimum necessary for the performance of their duties.

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.

Workforce members shall not leave portable media that contains EPHI visible in their vehicles or in any other unsecured location.

If portable media is lost, workforce members are responsible to immediately notify their supervisor.

7.3.3 Electronic 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. Mobile devices shall have all stored EPHI erased or shall be physically destroyed.
3. Storage media, such as backup tapes, USB flash drives and CDs, shall be physically destroyed (broken into pieces) before disposing of the item.

7.3.4 Electronic 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 IT 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.

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

Policy 8: Audit Controls

Issue Date: August 8, 2017
Effective Date: August 8, 2017
Revised Date: n/a

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 El Dorado Information Technology (IT) 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, IT support shall provide audit logs, activity reports, or other mechanisms for indications of improper use to department designated personnel for review.
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 IT 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 IT support to ensure user and system activity reports provide sufficient information to determine if improper use of EPHI has occurred.
2. Work with IT 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: August 8, 2017
Effective Date: August 8, 2017
Revised Date: n/a

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

All security incidents, threats to, or violations of, the confidentiality, integrity or availability of electronic protected health information (EPHI) shall be reported and responded to promptly.

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

1. EPHI data loss due to disaster, failure, error, theft
2. Loss of any electronic media that contains EPHI
3. Loss of the integrity of EPHI
4. Malicious code attacks
5. Persistent network or system intrusion attempts from a particular entity
6. Unauthorized access to EPHI, an EPHI based system or network
7. Facility incidents, including but not limited to:
   - Unauthorized person found in a HIPAA covered component's facility
   - Facility break-in
   - Lost or stolen key, 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 Information Technology (IT) Help Desk at 621-5696. The IT Service Desk will evaluate the situation to determine if it is a potential security incident, and initiate the response process as required by the type of incident.

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

If the security involves any breach of EPHI, the manager or supervisor shall notify the HIPAA Privacy Officer, in addition to notifying the IT Help Desk.

9.3.2 Incident Response and Resolution

The IT Help 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 IT staff that provides anti-virus support.

The IT staff receiving the security incident service request shall perform their assigned responsibilities to respond to and/or mitigate any incident consequences. The IT staff responsible for determining if a possible EPHI breach has resulted from the incident shall notify the HIPAA Privacy Officer.

The HIPAA Privacy Officer and HIPAA Security Officer shall evaluate the incident to determine if a breach of EPHI occurred. If it is determined that a breach has occurred, the HIPAA Privacy Officer, shall contact County Counsel, law enforcement, Human Resources, or the County Communication Manager when it is deemed necessary.

The HIPAA Privacy Officer shall coordinate any mandated notification process due to a confirmed breach of EPHI with the HIPAA Security Officer.

9.3.3 Incident Logging

All HIPAA security related incidents and their outcomes will be logged by the IT Help Desk and documented by the assigned IT support staff. The HIPAA Privacy Officer and HIPAA Security Officer shall document and log incidents and outcomes that they review and investigate.

Each fiscal quarter, the assigned IT support staff shall provide the HIPAA Privacy Officer with a record of all the incidents logged. The HIPAA Privacy Officer retains these incident reports for six years.

9.4 Policy Responsibilities:

9.4.1 Workforce Member Responsibilities

Workforce members are responsible to promptly report any potential security related incident to their manager or supervisor, or directly to the IT Help Desk at 621-5696.

9.4.2 Supervisor and Manager Responsibilities

1. Ensure that the IT Help Desk and the HIPAA Privacy Officer are notified of any security incident.
2. Ensure that the facility manager is notified of any facility related incident as described in Section 9.3.1.7.

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 IT Help Desk Responsibilities

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

9.4.5 IT Support Team Responsibilities

1. Perform their assigned duties to investigate, respond to, and/or mitigate any incident consequences.
2. Notify the HIPAA Privacy Officer when a breach of EPHI is suspected or may have occurred.
3. Provide a report to the HIPAA Privacy Officer quarterly, to be retained for 6 years.

9.4.6 HIPAA Security Officer and HIPAA Privacy Officer Responsibilities

1. The HIPAA Privacy Officer is responsible to determine if the incident requires further investigation and if it is a breach of EPHI. Working with the HIPAA Security Officer, the HIPAA Privacy Officer shall determine if corrective actions should be implemented.
2. HIPAA Privacy Officer is responsible for documentation of EPHI breach investigations and any corrective actions.
3. HIPAA Privacy Officer is responsible for maintaining all documentation on EPHI breaches for a minimum of 6 years.
4. The HIPAA Privacy Officer shall coordinate any mandated notification process due to a confirmed breach of EPHI with the HIPAA Security Officer.

Policy 10: Transmission Security

Issue Date: August 8, 2017
Effective Date: August 8, 2017
Revised Date: n/a

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, 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

Proven, standard algorithms shall be used as the basis for encryption technologies. The use of proprietary encryption algorithms is not allowed for any purpose unless authorized by the Information Security Officer (ISO).

10.3.1.1 Encryption Required

1. No EPHI shall be sent outside the County of El Dorado Wide Area Network (WAN) 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 WAN, no encryption is required.

10.3.3 EPHI Transmissions Using Wireless LANs

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
    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 WAN at the same time. Wireless access capability must be disabled on any device that is connected to the WAN.

10.3.4 Perimeter Security

1. Any external connection to the WAN shall come through the perimeter security's managed point of entry.
2. If determined safe by the Information Security Officer, 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 Information Security Officer.
4. All workforce members connecting to the WAN shall sign the El Dorado County General Network Usage 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 Information Security Officer for review and approval.

10.4 Policy Responsibilities:

10.4.1 Workforce Member Responsibilities

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

10.4.2 IT Support Responsibilities

The County of El Dorado Information Security Officer is responsible for the perimeter security architecture, its resources, its periodic auditing, and testing.

Policy 11: Protection from Malicious Software

Issue Date: August 8, 2017
Effective Date: August 8, 2017
Revised Date: n/a

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 El Dorado's HIPAA covered components shall ensure all workstations (owned, leased, and/or operated by the HIPAA covered components), install and maintain current anti-virus software. 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 Help Desk if a virus is suspected, as explained in **Section 9.3.1 Incident Reporting**.

11.4.2 IT Support Responsibilities

1. Maintain current anti-virus software on all HIPAA covered component workstations.
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.

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 IT 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: August 8, 2017
Effective Date: August 8, 2017
Revised Date: n/a

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) 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:

- IT Service Catalog (included in Continuity of Operations Plan)
- Disaster Recovery Plan
- Business Continuity Plan (included in Continuity of Operations Plan)

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

12.3.1 IT Service Catalog

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 Disaster Recovery Plan and Business Continuity Plan.
2. Each HIPAA covered component shall identify critical business functions, define impact scenarios, and determine resources needed to recover from each impact.

12.3.3 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, IT 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 Business Continuity 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.
3. All EPHI shall be stored on network servers in order for it to be automatically backed up by the system.
4. EPHI shall not be saved on the local (C:) drive of any workstation.
5. EPHI stored on portable media shall be saved to the network to ensure backup of the EPHI.
6. IT 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.
7. The Data Backup Plan shall apply to all files that may contain EPHI.
8. The Data Backup Plan shall require that all media used for backing up EPHI be stored in a physically secure environment.
9. 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.

12.4 Policy Responsibilities:

12.4.1 Manager and Supervisor Responsibilities

1. Develop and document a Business Continuity 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 IT Support Responsibilities

1. Establish, implement and document the Business Continuity 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.

Policy 13: Business Associate

Issue Date: August 8, 2017
Effective Date: August 8, 2017
Revised Date: n/a

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 El Dorado 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 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 decision tool is completed.
3. Every decision tool 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 HIPAA Privacy Officer shall maintain a database of all County Business Associates. This information shall be provided to the HIPAA Privacy Officer in a semi-annual report by El Dorado County Contracts and Procurement and by the Contract Divisions of the HIPAA covered components.

The Contract Divisions of the HIPAA covered components shall provide the HIPAA Privacy Officer 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 El Dorado 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 Privacy 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 HIPAA Privacy Officer 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 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 Privacy 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 Business Associate Decision Tool is completed.
2. Ensure the completed HIPAA Business Associate Decision Tool is provided to County Counsel for review and final determination before the contract is signed.
3. Provide the HIPAA Privacy Officer 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 Business Associate Decision Tool is completed.
2. Provide the HIPAA Business Associate Decision Tool to County Counsel for review and final determination before the contract is signed.
3. Provide the HIPAA Privacy Officer with semi-annual notification of all Business Associate agreements managed by Procurement and Contracts.

13.4.5 HIPAA Privacy Officer Responsibilities

1. Maintain a database of all County HIPAA Business Associates.
2. Coordinate, as assigned 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 Business Associate Decision Tool forms for final determination of Business Associate status before a contract is signed.

Policy 14: Risk Analysis and Management

Issue Date: August 8, 2017
Effective Date: August 8, 2017
Revised Date: n/a

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 HIPAA Privacy Officer 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 HIPAA Privacy Officer:

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 IT 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.

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

14.4 Policy Responsibilities:

14.4.1 IT Support Responsibilities

1. Inform the HIPAA Privacy Officer 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 for all alterations that occur in the information systems that support, contain, or protect EPHI.

14.4.2 HIPAA Privacy Officer

HIPAA Privacy Officer is responsible for risk analysis activities as indicated in **Section 14.3.1**

Policy 15: Security Awareness and Training

Issue Date: August 8, 2017
Effective Date: August 8, 2017
Revised Date: n/a

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 logon and log off the application containing EPHI.
3. Instructions on contacting a manager or supervisor or IT Help 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 IT Help Desk.
5. Instructions regarding internet security, virus protection, password security and confidential data handling.

15.4.2 County HIPAA Security Policies and Procedures

The HIPAA Privacy Officer 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 year.

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

15.4.3 HIPAA Security Reminders

The Privacy Officer, in coordination with the HIPAA covered components and the County Security Officer, 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 HIPAA Privacy Officer within 60 days of the workforce member assuming their position in the HIPAA covered component.

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; shall sign the HIPAA Privacy and Security Practices Acknowledgment Form; and provide the signed form to their supervisor or to the HIPAA Privacy Officer.
2. Temporary agency workforce members, volunteers, and contracted workers that access EPHI are required to provide the HIPAA Privacy Officer a signed copy of the HIPAA Privacy and Security Practices Acknowledgment Form.

15.5.3 HIPAA Privacy Officer Responsibilities

1. The HIPAA Privacy Officer has oversight responsibility to audit reports to ensure required workforce member attendance. The HIPAA Privacy Officer may require workforce members to attend more training if security incidents warrant this remedial action.
2. The HIPAA Privacy Officer or its designee shall provide HIPAA security training, track completion of the training, and maintain training records for a minimum of six years.
3. The HIPAA Privacy Officer, in coordination with the HIPAA covered components and the HIPAA Security Officer, shall provide periodic security reminders to HIPAA covered component workforce.

Policy 16: Sanctions

Issue Date: August 8, 2017
Effective Date: August 8, 2017
Revised Date: n/a

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 El Dorado HIPAA covered component workforce who violate County of El Dorado HIPAA Security Policies and Procedures regarding the safeguarding of electronic protected health information (EPHI) are subject to disciplinary action by County of El Dorado 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 El Dorado 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 El Dorado 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, or the HIPAA Privacy 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 El Dorado as an entity nor any member of the County of El Dorado 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 El Dorado 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 El Dorado 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 El Dorado 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 Privacy Officer 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, 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	164.380(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	164.308(b)(1)	13

Arrangements		
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

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.

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.

Appendix C – IT Change Management Policy

Contents

PURPOSE

Change Management is the process of planning, coordinating, implementing and monitoring changes affecting any production platform within Information Technology's control. The objectives of the Change Management process are to:

- Ensure that changes are made with minimum disruption to the services IT has committed to its users.
- Support the efficient and prompt handling of all changes.
- Provide accurate and timely information about all changes.
- Ensure all changes are consistent with business and technical plans and strategies.
- Ensure that a consistent approach is used.
- Provide additional functionality and performance enhancements to systems while maintaining an acceptable level of user services.
- Reduce the ratio of changes that need to be backed out of the system due to inadequate preparation.
- Ensure that the required level of technical and management accountability is maintained for every change.
- Monitor the number, reason, type, and associated risk of the changes.

The Change Management procedure for El Dorado County Information Technology defines how the change process is implemented in all of the IT platform environments. The objectives of the operating procedures, in addition to those detailed above are to:

- Provide documentation that allows El Dorado County IT management to understand, at any point in time, the configuration of the IT environment.
- Minimize the bureaucratic impact on the development community while maintaining control of the environment.

DEFINITIONS OF TERMS

Change - Any installation or alteration to hardware, network, system or application software, procedure or environmental facilities which adds to, deletes from or modifies the service delivery environment. The need for changes arises both proactively and reactively for a variety of reasons:

- Proactively (for example, seeking business benefits such as reducing costs, improving services, or increasing the ease and effectiveness of support)
- Reactively as a means of resolving errors and adapting to changing circumstances

Change Initiator – The change initiator is the person who initially perceives the need for the change and develops, plans, and executes the steps necessary to meet the initial requirements for a Request for Change (RFC). The change initiator must coordinate testing and validation of the change for technical and business requirement completeness and submit proposed RFC to process owners, subject matter experts or peers for technical review and signoff. The change initiator is responsible for submitting RFC to the CAB.

Some examples of change initiators are:

- A product manager in a line of business desiring a new or changed feature on an application
- A network architect replacing obsolete network hardware with newer-generation hardware with improved functionality

• A network engineer upgrading the capacity of a device or link to handle increased traffic
• A service manager who discovers a change in vendor contacts or procedures and must update documentation
• A Tier 1, 2, or 3 support engineer who needs to replace a defective part in a network element
• A security manager requesting a configuration and documentation change in response to a newly discovered vulnerability

Change Manager – The Change Manager has overall responsibility for ensuring the quality of the Change Management process. Specific Change Manager Responsibilities include:

- Is responsible for and owns the Change Management service
- Is responsible for development and implementation of Change Management mission and strategy, in line with El Dorado County and IT strategies
- Leading a team to review and accept completed change requests
- Managing and conducting periodic change review meetings
- Auditing information systems changes to ensure that:

– Change was recorded correctly with work matching the RFC
– Change had appropriate risk level
– Configuration items were updated appropriately
– Documentation was updated appropriately

- Managing change postmortems
- Escalates to senior management exceptions as appropriate
- Ultimately responsible for resolving Change Management service dissatisfaction
- Ensures compliance with Change Management process standards and procedures
- Has a change process co-owner to cover for service owner absence
- Communicates Change Management service procedures and working practices and changes to internal standards, processes, procedures and technology
- Approves and sponsors Change Management improvement ideas

Change Advisory Board (CAB) – The change advisory board (CAB) is a body that exists to support the authorization of changes and to assist change management in the assessment and prioritization of changes. When a CAB is convened, members should be chosen who are capable of ensuring that all changes within the scope of the CAB are adequately assessed from both a business and a technical viewpoint. To achieve this, the CAB needs to include people with a clear understanding across the whole range of stakeholder needs. The change manager will normally chair the CAB. Typically, there are "standing" members on the CAB, and the change manager will recruit others as needed in order to ensure stakeholder representation. Potential members include:

• Customers
• User managers
• User group representatives
• Applications developers/maintainers
• Specialists/technical consultants
• Services and operations staff, such as service desk, test management, continuity management, security, and capacity

• Facilities/office services staff (where changes may affect moves/accommodation and vice versa)
• Contractors' or third parties' representatives, in outsourcing situations, for example
• Other parties as applicable to specific circumstances

Change Implementer– The change implementer is responsible for performing the implementation plan, and post implementation test plan as outlined in the RFC within the scheduled time approved by the change management process, determining whether the change is successful, resolving problems during implementation or initiating the back out plan, and reporting results to change management. The change implementer may work alone, or in coordination with a team, with the designated change implementer taking ownership of the implementation process.

CHANGE MANAGEMENT PROCEDURES AND GUIDELINES

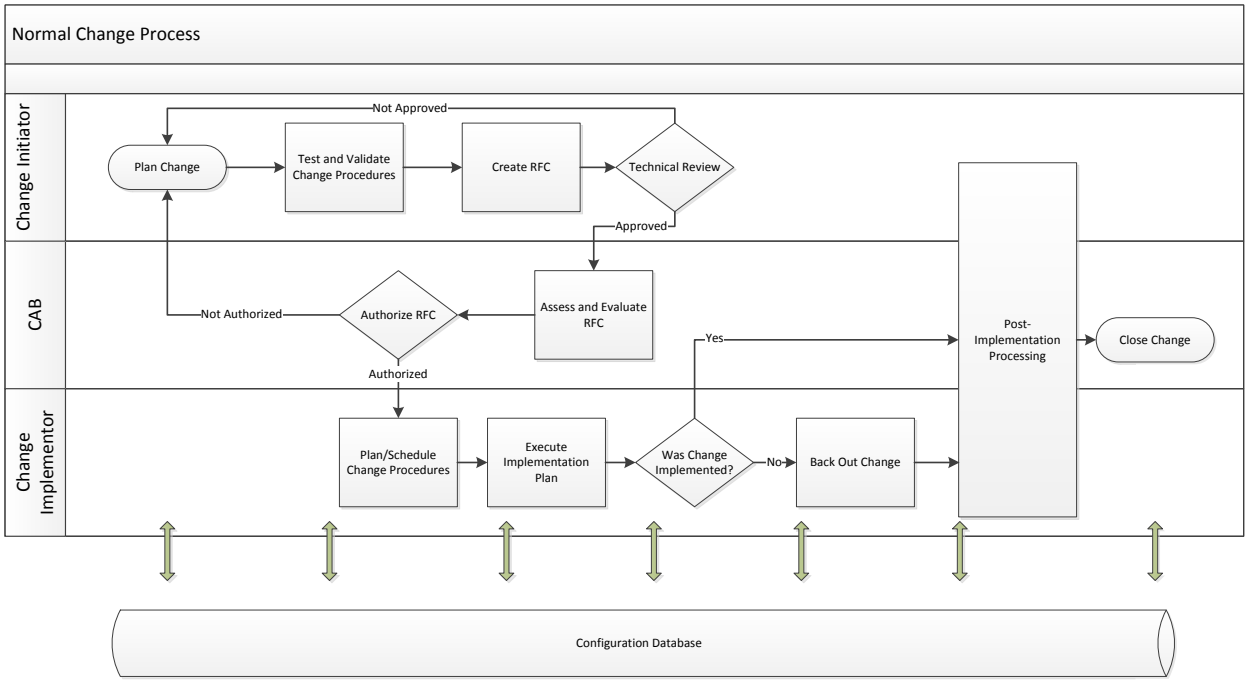
Change Categories and Workflows

Changes will be categorized based on several factors and will determine the change process model used to gain approval and implement the proposed change. Changes should be evaluated on the basis of impact, urgency and risk. There are four categories of change:

- Normal Change
- Standard Change
- Expedited Change
- Emergency Change

Normal Change

A normal change is any change that is not categorized as a standard or emergency change. The following activities are part of the normal change process flow. A subset of these activities will be used in other types of changes, such as standard or emergency.



Plan the Change

Once the requirement for a change has been determined, the change is planned in terms of schedule and necessary resources, such as testing environment and time, personnel, budget, etc.

Test and Validate the Change

The testing starts with a summary laboratory validation of the proposed change. The goals of this test are to assess the feasibility and the costs (effort, resources) of the change. The testing should include procedures to install the proposed change, to back out from the change in the event it cannot be successfully implemented, and to verify the success of the change after it has been implemented. A complete back-out or remediation plan must be

documented, including procedures to back out at various stages of the change for each change deemed risky enough to require it. The need for a back-out plan, from a process standpoint, is usually tied to the level of risk calculated for a given change. The plan must also include a verification procedure to check that the environment has been restored to the initial configuration that existed prior to the change attempt and that there are no negative side effects resulting from the attempted change.

Document/Create the Request for Change

All the procedures for preparation, installation, verification, and back-out must be documented in detail. Impact and risk analysis of the change must also be recorded, in particular the worst-case impact, analyzing the situation of a failed change and a failed back-out procedure. Other information related to the change must also be included in the documentation, such as prerequisites for the change, proposed schedule, required resources, engineering and design documentation, physical diagrams, etc. The RFC is then completed, with references to additional documentation as required.

Technical Review and Signoff

Generally the change management (CAB) assessment of the RFC does not include a review of the technical content of the change. Consequently, prior to submitting the RFC for CAB review, each RFC must undergo a technical review. This review checks the following aspects of the proposed change:

- Correctness of all technical information, including preparation, implementation, verification, and back-out procedures
- Completeness of change, testing procedures, and documentation
- Feasibility of the change
- Potential side effects and impact on other services or infrastructure
- Worst-case impact (both change and back-out procedure fail)

This review is performed by the technical resources familiar with the area affected by the change as well as other technical resources with general knowledge, such as architects, service managers, etc. It is important that authorization following the technical review is a formal sign-off recorded in the change log.

Review the RFC

Change management should briefly consider each request and filter out any that seem to be:

- Totally impractical
- Repeats of earlier RFCs
- Inadequate documentation and plan
- Incomplete submissions, such as those with an inadequate description, or without necessary budgetary approval or justification

These should be returned to the initiator, together with brief details of the reason for the rejection, and the log should record this fact.

Assess and Evaluate the RFC

Changes accepted for review are assessed and evaluated at the CAB meeting for potential impact to services and assets. Considerations will include:

- Who raised the change?
- What is the reason for the change?
- What is the return required from the change?
- What are the risks involved in the change?
- What resources are required to deliver the change?
- Who is responsible for the building, testing, and implementation of the change?
- What is the relationship between this change and other changes?
- The impact that the change will make on:
  - The customer's business operation
  - The infrastructure and customer service
  - Other services that run on the same infrastructure
  - Continuity planning, capacity planning, security planning
- The effect of not implementing the change
- The resources required to implement the change
- The current change schedule and projected service outage (PSO)
- Additional ongoing resources required if the change is implemented

All members of the change authority should evaluate the change based on impact, urgency, risk, benefits, and costs. Each will indicate whether they support approval and be prepared to argue their case for any alterations that they see as necessary. In particular, subject matter experts (SMEs) in a particular discipline must evaluate the potential impact of the change on their area of expertise. For example, network SMEs are charged to examine the effect of the change on network resiliency, performance, and security.

Authorize the Change

After review, the CAB can authorize or reject the change. If consensus among the board is not achieved, the change manager will make the ultimate determination. Upon approval, the implementation is scheduled, and notice given to the change initiator and change implementer. Rejected RFC's will be returned to the initiator, together with brief details of the reason for the rejection, and the log should record this fact.

Plan/Schedule the Change

Authorized RFC's are scheduled with change management coordinating with change implementer and change is entered into the maintenance calendar, with consideration of impacts of potential service outage. It is the responsibility of the change implementer to initiate and coordinate the communication plan.

Implement the Change

The change implementer is responsible for executing the implementation plan and the post implementation plan, and remediating any deficiencies in service delivery. Remediation procedures should be prepared and documented in advance for each authorized change so that if errors occur during or after implementation, these procedures can be quickly

activated with minimum impact on service quality. If remediation efforts are unable to restore service to an acceptable level, then the change implementer shall invoke the back out plan. Should the back out plan also fail to restore service, the change implementer shall escalate the incident to I.T. management. Implementation status will be communicated with change management.

Post Implementation Review

On completion of the change, the results should be reported for evaluation to those responsible for managing changes, and should also include any incidents arising as a result of the change. A post-implementation review will be carried out at the next meeting of the CAB to confirm that the change has met its objectives, that the initiator and stakeholders are happy with the results, and that there have been no unexpected side effects. Lessons learned should be factored into future changes. The purpose of such reviews is to establish that:

- The change has had the desired effect and met its objectives
- Users, customers, and other stakeholders are content with the results (if not, the review should identify any shortcomings)
- There are no unexpected or undesirable side effects to functionality, service levels, or warranties, such as availability, capacity, security, performance, and costs
- The resources used to implement the change were as planned
- The release and deployment plan worked correctly (the review should include comments from the implementers)
- The change was implemented on time and to cost
- The remediation plan functioned correctly, if needed

Where a change has not achieved its objectives, change management (or the CAB) should decide what follow-up action is required, which could involve raising a revised RFC. If the review is satisfactory or the original change is abandoned (for example, when the circumstances that required the change are no longer current and the requirement disappears) the RFC should be formally closed in the logging system.

Close the Change

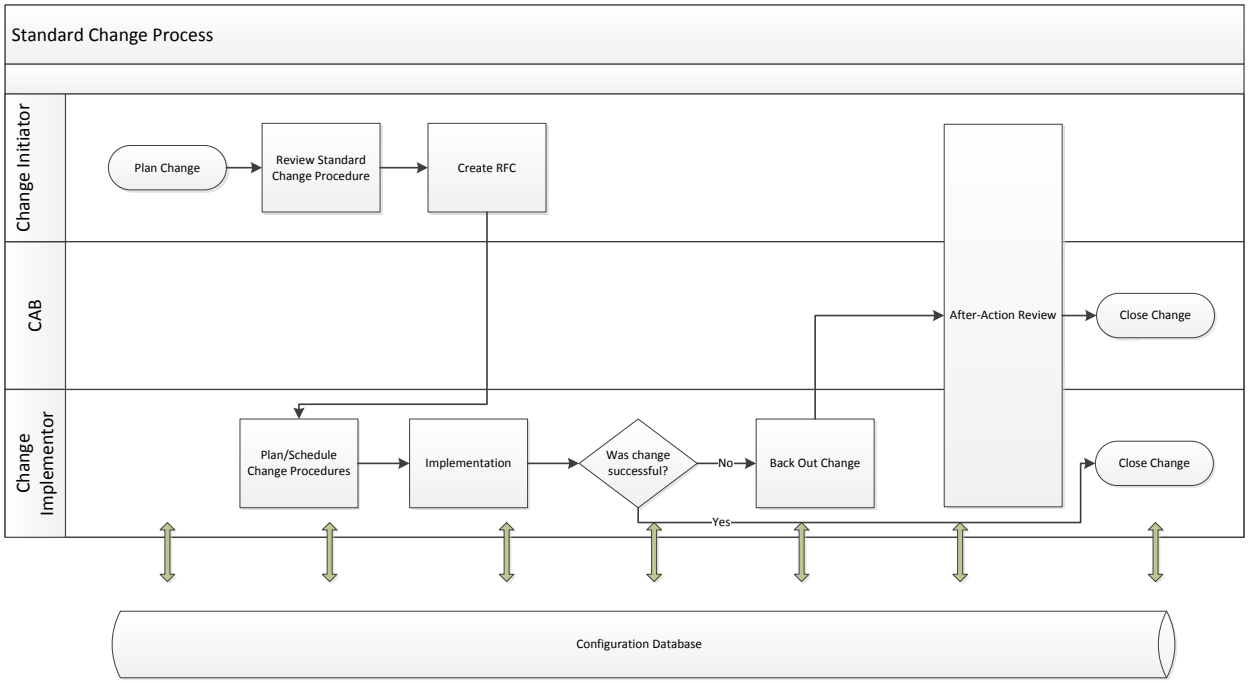
The change is closed and documented in the configuration database. It is important to note that every step of the change process and every status change of the RFC must be documented in the configuration database. The change success, failure, related plans, etc. are communicated to all stakeholders.

Standard Change

A standard change is a change to a service or infrastructure for which the approach is preauthorized by change management. A standard change has an accepted and established procedure to provide a specific change requirement.

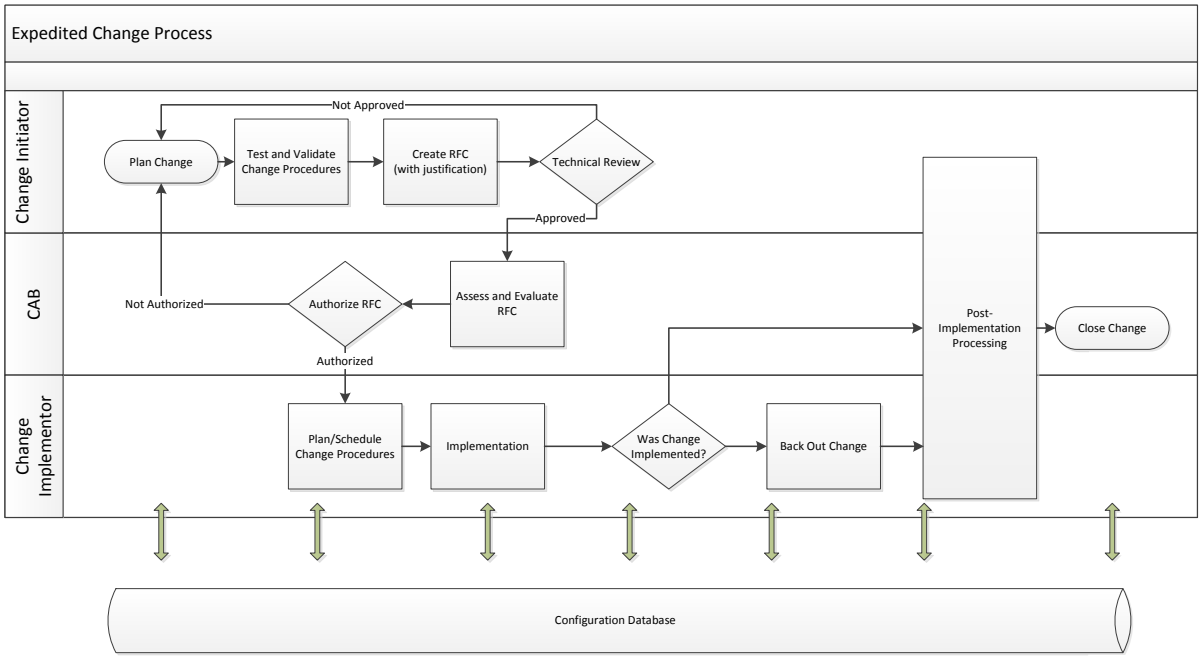
- The crucial elements of a standard change are that:
- Approval of a standard change will be granted by the delegated authority for that change
- There is a defined trigger to initiate the RFC

• The tasks are well known, documented, and proven, and documented procedure has been pre-approved by the CAB
• Authority is effectively given in advance
• Budgetary approval will typically be preordained or within the control of the change requester
• The risk is usually low and always well understood



Expedited Change

An expedited change is a normal change that must be implemented in the shortest possible time for business or technical reasons. The expedited change process is the same as a normal change, however the change management review and approval process can be expedited via email with the change manager who will coordinate with other CAB members to determine approval, instead of waiting for the next CAB meeting.

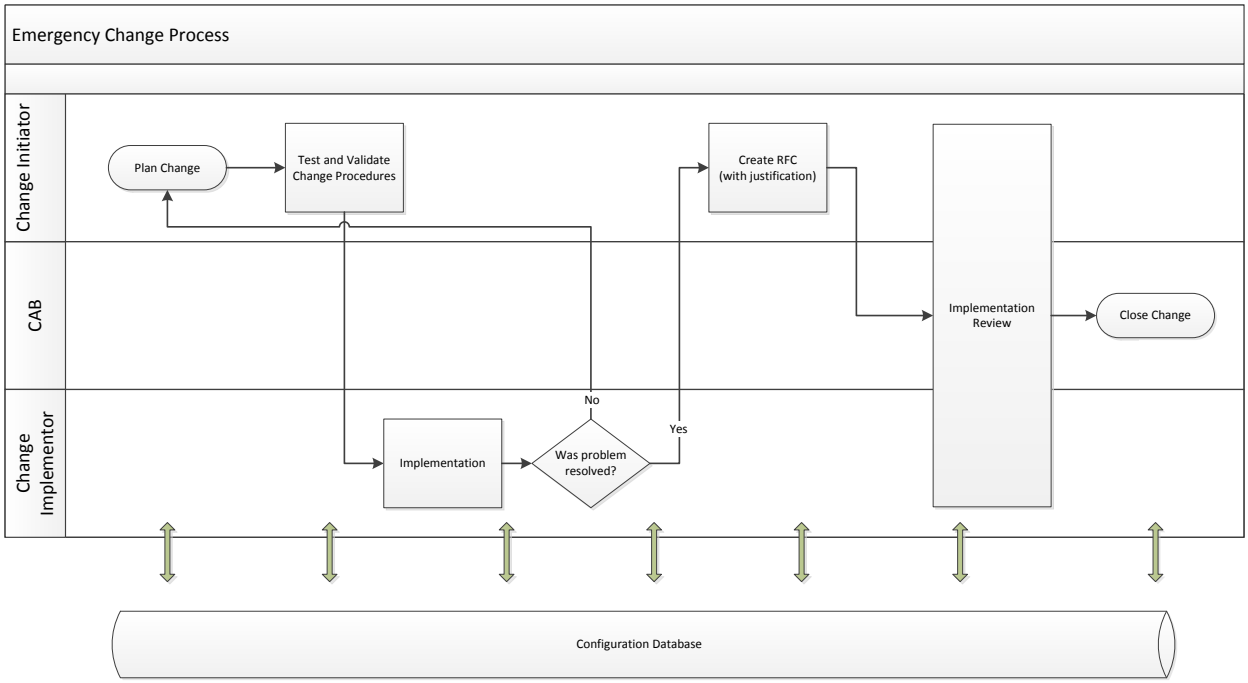


Emergency Change

Emergency changes are usually initiated in response to a critical IT situation, often an incident or problem requiring immediate action to restore service or prevent service disruption. Emergency changes are sometimes required and should be designed carefully and tested before use or the impact of the well-intended but errant emergency change may be greater than the original incident. The number of emergency changes proposed should be kept to an absolute minimum, because they are generally more disruptive and prone to failure with corresponding negative impacts to network and service availability.

Effectively, the emergency change procedure will follow the normal change procedure except that:

- Approval will be given by a supervisor, manager or the change manager.
- Testing may be reduced, or in extreme cases forgone completely, if considered a necessary risk to deliver the change immediately.
- Documentation, such as updating the change record and configuration data, may be deferred, typically until normal working hours.


Emergency Change Process
Change Initiator
CAB
Change Implementor
Plan Change
Test and Validate Change Procedures
Create RFC (with justification)
Implementation Review
Close Change
Implementation
Was problem resolved?
No
Yes
Configuration Database

County of El Dorado HIPAA Security Rule
Policies and Procedures

~END~