PLUMAS COUNTY
HIPAA SECURITY POLICY

Health Insurance Portability and Accountability Act (HIPAA)

Countywide

Security Rule
POLICIES & PROCEDURES

County of Plumas

County Administrative Office,
responsible for HIPAA oversight

Revised: January, 12 2006

County of Plumas Privacy Officer: The County Administrative Officer

Security Rule Officer: The County Administrative Officer

Table of Contents

PLUMAS COUNTY
HIPAA SECURITY POLICY

Authority

Plumas County is responsible for developing policies, standards, and guidelines, including minimum requirements, that provide adequate information security for all County of Plumas HIPAA covered components. Such standards and guidelines shall not apply to non-covered components of the County of Plumas. This guideline is consistent with the resolutions No. 03-6838 and No. 03-6864 declaring the County of Plumas to be a hybrid entity for complying with the HIPAA regulations.

The document has been prepared for use by the HIPAA covered components in the County of Plumas. It may be used by non-covered components of the County of Plumas on a voluntary basis.

Acknowledgments

This boilerplate of this policy document was originally developed by Sacramento County and has been significantly modified for use in Plumas County. Plumas County wishes to acknowledge the extensive efforts that Sacramento County undertook to develop such a document. The Plumas County editors wish to acknowledge the Health and Human Services Cabinet for their efforts in ensuring the relevance to their county and for this project to further the security and portability of health information.

The HIPAA Security Rule itself is a critical source of information for developing these policies and procedures. The United States Department of Health and Human Services published the final Security Rule in the Federal Register on February 20, 2003. Language taken from the rule is written in italics in this document.

The entire Security Rule can be found at:
http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/03-3877.pdf

Section 1: Introduction

This publication contains the County of Plumas HIPAA Security Rule policies and procedures and explains some of the structure and organization of the Security Rule.

This publication informs readers about decisions made by the County of Plumas to implement the Security Rule and to improve understanding of the security safeguards recommended in order to comply with the Rule.

The County Administrative Officer, functions as the HIPAA Privacy Officer and Security Officer and is responsible for overseeing policies, standards, and guidelines, including minimum requirements that provide adequate information security for all County of Plumas HIPAA covered components.

The policies, standards, and implementation specifications of these HIPAA Policies and Procedures apply to the following covered components in the County of Plumas:

Department of Drug and Alcohol
Department of Mental Health
Department of Health
Office of the County Administrative Officer
County Counsel

The objective of complying with the HIPAA Security Rule is to ensure there is an information security program in place and trained personnel assigned to manage and support the program.

Heavy emphasis is placed on fully integrating security in the business processes. Preparation of security plans and procedures are critical to meeting the objectives of the HIPAA Security Rule.

The HIPAA Security Rule specifically focuses on the safeguarding of electronic protected health information (ePHI). While all county departments should be concerned about information security, only a subset of departments is subject to the HIPAA Security Rule based on its use of ePHI. All covered entities under HIPAA shall comply with the Security Rule, which establishes a set of security standards for protecting certain health care information.

Congress enacted HIPAA to simplify and standardize health care administrative processes, thereby reducing costs and other burdens on the health care industry. The HIPAA statute is comprised of five Titles, some of which address health care industry concerns such as health care insurance coverage and health care finance. Title II, however, includes the HIPAA administrative simplification requirements that address how electronic health care transactions are transmitted and stored. Pursuant to these provisions of HIPAA, the Secretary of the US Department of Health and Human Services (HHS) adopted several sets of rules (in addition to the Security Rule) to implement the HIPAA administrative simplification requirements.

HHS has published proposed or final rules related to the following five components of health care industry practices:

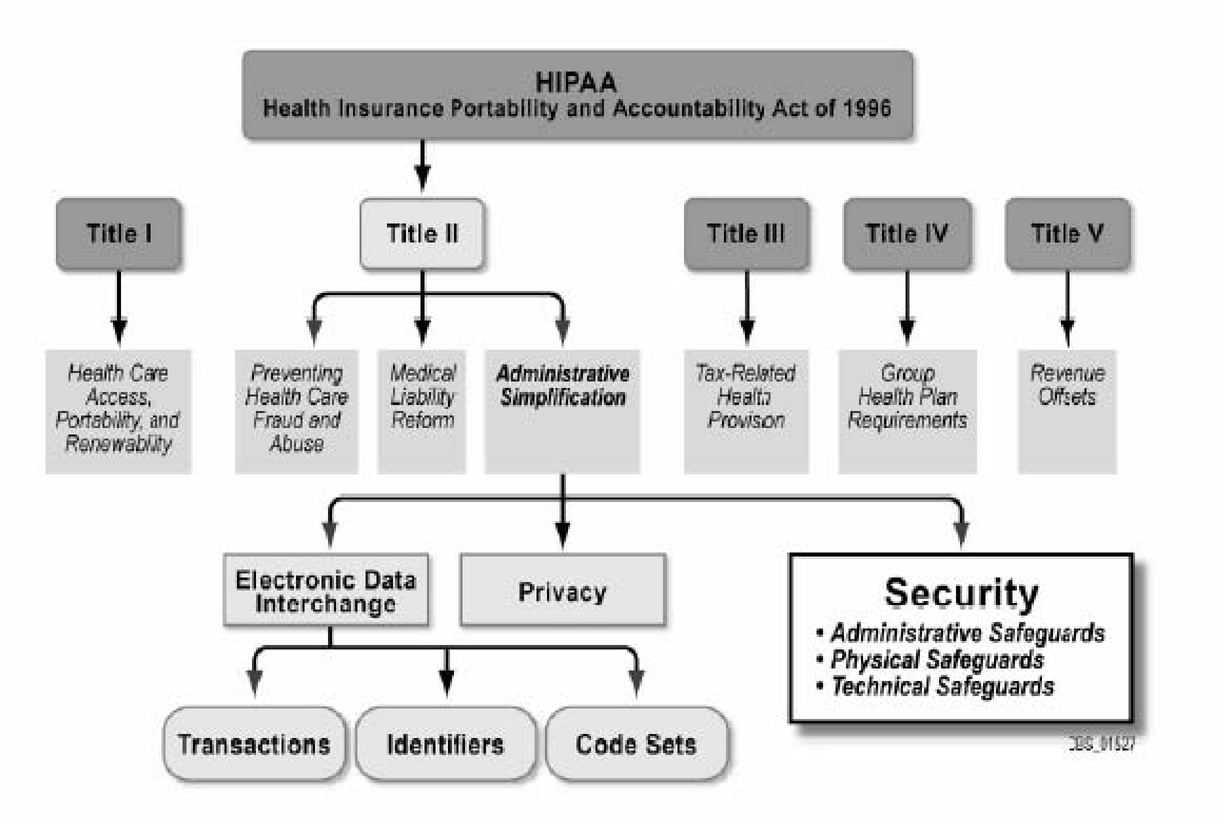
1 Code sets used to identify health care services
2 Identifiers used for unique designations for employers and health care providers
3 Electronic data interchange transactions
4 Security
5 Privacy

This document addresses only the security component of the HIPAA statute. Previously the Plumas County Administrative Officer published the policies and procedures for the privacy component of HIPAA.

The County of Plumas shall assure *"that the integrity, confidentiality, and availability of electronic protected health information it collects, maintains, uses, or transmits are protected. The confidentiality of health information is threatened not only by the risk of improper access to stored information, but also by the risk of interception during electronic transmission of the information."*

The purpose of these policies is to adopt standards for safeguards to protect the confidentiality, integrity, and availability of electronic protected health information.

The chart below shows all the components of HIPAA and illustrates that the focus of this document is on the security provision of the statute and the regulatory rule.


HIPAA
Health Insurance Portability and Accountability Act of 1996
Title I
Title II
Title III
Title IV
Title V
Health Care Access, Portability, and Renewability
Preventing Health Care Fraud and Abuse
Medical Liability Reform
Administrative Simplification
Tax-Related Health Provison
Group Health Plan Requirements
Revenue Offsets
Electronic Data Interchange
Privacy
Security
• Administrative Safeguards
• Physical Safeguards
• Technical Safeguards
Transactions
Identifiers
Code Sets
DS_01527

HIPAA Components

Organization of this publication

This publication is composed of the following sections and appendices.

Section 1 gives an overview of the purpose and identifies the intended audience.

Section 2 explains some of the key concepts included in the HIPAA Security Rule.

Section 3 contains the policies and procedures the County of Plumas uses to comply with the HIPAA Security Rule regulations.

Policy 1: Assigned Security Responsibility
Policy 2: User Access Management
Policy 3: Authentication & Password Management
Policy 4: Facility Access Controls
Policy 5: Workstation Access Controls
Policy 6: Device & Media Controls
Policy 7: Audit Controls
Policy 8: Security Incident Response & Reporting
Policy 9: Transmission Security
Policy 10: Protection from Malicious Software
Policy 11: Contingency Plan
Policy 12: Business Associate
Policy 13: Monitoring Effectiveness and Assurance
Policy 14: Security Awareness and Training
Policy 15: Sanctions
Policy 16: Policy Creation & Documentation

Appendix A provides a comparison of the HIPAA Security Rule to these policies

Appendix B maps the policies to the Security Rule components

Appendix C defines terms used in this document

Section 2: HIPAA Security Rule

The HIPAA Security Rule specifically focuses on the safeguarding of electronic protected health information (ePHI). While all county departments shall be concerned about information security, only a subset of departments is subject to the HIPAA Security Rule based on its use of ePHI. All covered entities under HIPAA shall comply with the Security Rule, which establishes a set of security standards for protecting certain health care information. This section summarizes the HIPAA security standards and explains some of the structure and organization of the Security Rule.

HIPAA Goals and Objectives

The main goal of the HIPAA Security Rule is to protect the confidentiality, integrity, and availability of electronic protected health information.

***Confidentiality** is "the property that data or information is not made available or disclosed to unauthorized persons or processes."*

***Integrity** is "the property that data or information has not been altered or destroyed in an unauthorized manner."*

***Availability** is "the property that data or information is accessible and usable upon demand by an authorized person."*

Security Rule Organization

To understand the requirements of the HIPAA Security Rule, it is helpful to be familiar with the basic security terminology it uses to describe the security measures. By understanding the requirements and the terminology in the HIPAA Security Rule, it becomes easier to see how the policies and procedures work. Each security measure of the HIPAA Security Rule can be categorized as being an administrative, physical, or technical safeguard.

***Administrative Safeguards** are defined as the "administrative actions, policies, and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information."*

***Physical Safeguards** are defined as the "security measures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion."*

***Technical Safeguards** are defined as "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it."*

Each security safeguard can also be categorized as being either a standard or an implementation specification. An "implementation specification" is a more detailed description of the method or approach covered entities can use to meet a particular standard.

Each set of safeguards is composed of a number of specific implementation specifications that are either required or addressable. If an implementation specification is described as required, the specification shall be implemented. If it is addressable, then the covered entity shall assess whether each implementation specification is a reasonable and appropriate safeguard in its environment. The County of Plumas has chosen to implement all specifications as if required after an assessment of its security environment.

Safeguards included in the HIPAA Security Rule

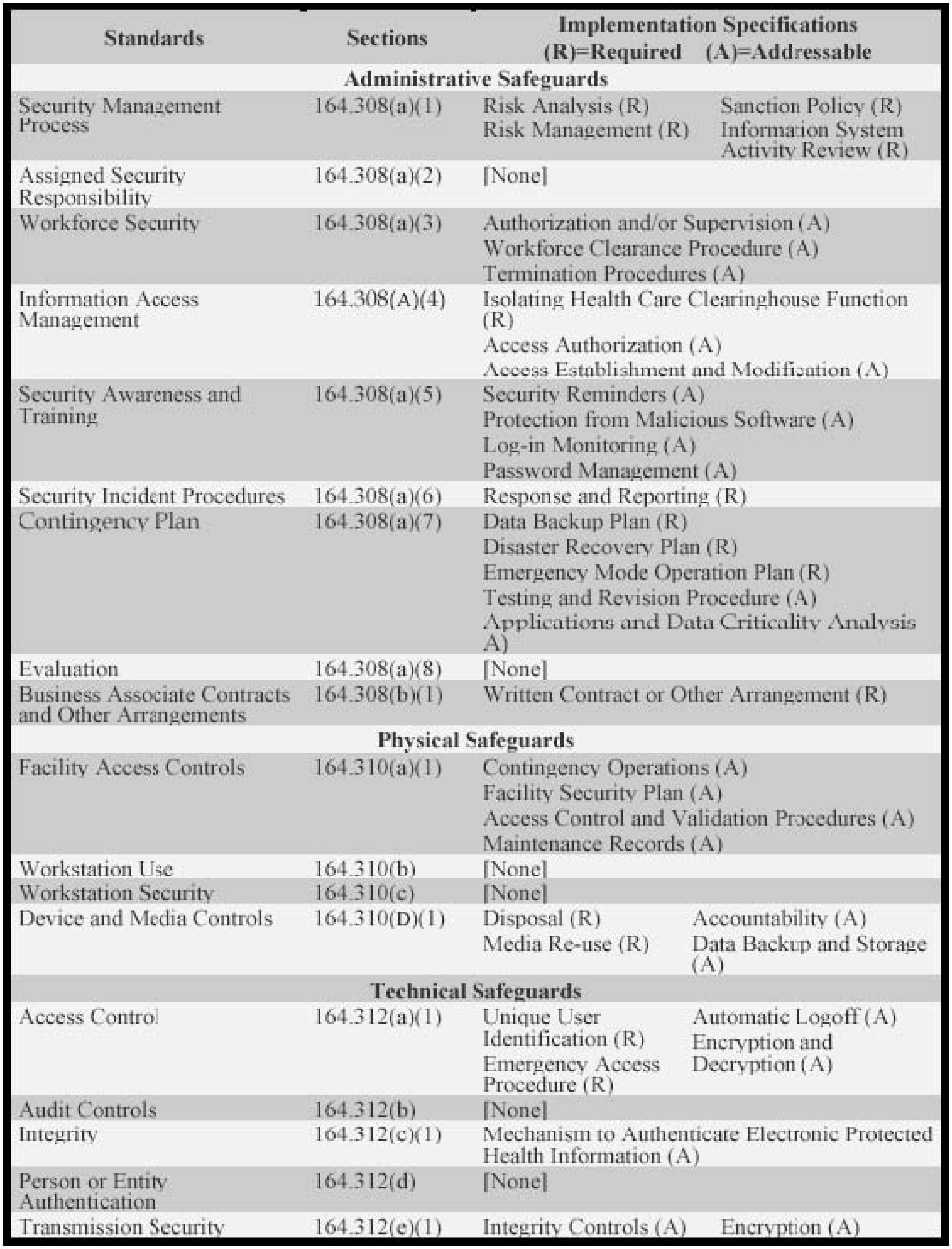
The next table lists the safeguards of the HIPAA Security Rule. This table provides a quick reference of the standards and implementation specifications of the Security Rule categorized by administrative, physical, or technical safeguards. Column 1 of the table lists the HIPAA standard, column 2 indicates the relevant section of the Security Rule where the standard can be found, and column 3 lists the implementation specification. These categories of safeguards encompass the continuum of security for electronic health care information for covered entities under HIPAA.

The security process begins with the policies and procedures that establish workforce behavior and provides a framework for acceptable access to and uses of protected health information.

The administrative controls are the foundation for the HIPAA Security Rule.

The physical safeguards support limitations to restricted spaces and equipment, Including materials that contain electronic protected health information.

The technical safeguards apply controls specifically to information systems and are measures of protection associated with the actual hardware, software, and networks for these systems.



Standards	Sections	Implementation Specifications (R)=Required (A)=Addressable
Administrative Safeguards		
Security Management Process	164.308(a)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	[None]
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A) Workforce Clearance Procedure (A) Termination Procedures (A)
Information Access Management	164.308(A)(4)	Isolating Health Care Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis A)
Evaluation	164.308(a)(8)	[None]
Business Associate Contracts and Other Arrangements	164.308(b)(1)	Written Contract or Other Arrangement (R)
Physical Safeguards		
Facility Access Controls	164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)
Workstation Use	164.310(b)	[None]
Workstation Security	164.310(c)	[None]
Device and Media Controls	164.310(D)(1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)
Technical Safeguards		
Access Control	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)
Audit Controls	164.312(b)	[None]
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	[None]
Transmission Security	164.312(e)(1)	Integrity Controls (A) Encryption (A)

COUNTY of PLUMAS

HIPAA SECURITY RULE

COUNTYWIDE

POLICIES & PROCEDURES

Policy 1: Assigned Security Responsibility

1.1 HIPAA Regulation:

Assigned security responsibility

1.2 Policy Purpose:

At all times the County of Plumas 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 and has the ultimate responsibility for ensuring HIPAA Security Rule policies are implemented and followed. Responsibilities include:

1.3.1 Ensure that the necessary and appropriate HIPAA related policies are developed and implemented by the departments to safeguard the integrity, confidentiality, and availability of electronic protected health information (ePHI) within the covered entity.

1.3.2 Ensure that the necessary infrastructure of personnel, procedures and systems is in place:

1. to develop and implement the necessary HIPAA related policies,
2. to monitor, audit and review compliance with all HIPAA related policies,
3. to provide a mechanism for reporting incidents and HIPAA security violations.

1.3.3 Act as a spokesperson and single point of contact for Plumas County in all issues related to HIPAA security.

1.4 Policy Responsibilities:

The above HIPAA Security Officer responsibilities are assigned to the County Administrative Officer for the County of Plumas.

The HIPAA Security Officer shall carry out the assigned responsibilities in coordination with the Director of IT who acts as the Systems Security Officer.

The remainder of this policy document left intentionally blank.

Policy 2: User Access Management

2.1 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

2.2 Policy Purpose:

The intent of this policy is to establish rules for authorizing access to the computing network, applications, workstations, and to areas where ePHI is accessible. Workforce members shall have authorization when working with ePHI or when working in locations where it resides. Workforce security includes ensuring that only workforce members who require access to ePHI for work related activities shall be granted access and that when work activities no longer require access, authorization shall be terminated. In addition, this policy provides guidelines on how user access is routinely reviewed and updated.

The definition of the County of Plumas covered entity workforce is taken from the Privacy Rule. In Section 160.103, of the Privacy Rule, the term "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."*

2.3 Policy Description:

2.3.1 Management and Access Control

Only the workforce member's supervisor or manager can grant 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.

2.3.2 Minimum Necessary Access

Each covered component shall ensure that only workforce members who require access to Electronic Protected Health Information (ePHI) are granted access. Each supervisor or manager is responsible for ensuring that the access to ePHI granted to each of his or her subordinates is the minimum necessary access required for each subordinate's job role and responsibilities. If the user no longer requires access, it is the supervisor or manager's responsibility to complete the necessary process to terminate access.

2.3.3 Granting Access to ePHI

2.3.3.1 Screen Workforce members Prior to Access

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

2.3.3.2 Sign Security Acknowledgement

Prior to being issued a User ID or log on account to access any ePHI, each workforce member shall sign the Employee Acknowledgement Form before access is granted to the network or any application that contains ePHI, and thereafter shall comply with all County of Plumas security policies and procedures.

2.3.3.3 Security awareness prior to getting access

Before access is granted in any of the various systems or applications that contain ePHI, workforce members shall be trained to a minimum standard including:

A. Proper uses and disclosures of the ePHI stored in the systems or application;
B. How to properly log on and log off the systems or application;
C. Protocols for correcting user errors;
D. Instructions on contacting a designated person or help desk when ePHI may have been altered or destroyed in error; and
E. Reporting a potential or actual security breach.

2.3.3.4 Management Approval

Each covered component shall implement the following policies:

A. User IDs or log-on accounts can only be assigned with management approval or by an appropriate designee.
B. Managers or their designees are responsible for requesting the appropriate level of computer access for staff to perform their job function.
C. All requests regarding User IDs or computer system access for workforce members are to be communicated to the appropriate system administrator by completing the required form(s) for covered components. All requests shall be made in writing (which may be in an electronic format).
D. System administrators are required to process only those requests that have been authorized by managers or their designees.
E. A written record of the authorized request is to be retained by the system administrator for a minimum of 1 year.

2.3.4 Granting Access in an Emergency

2.3.4.1 Emergency user access

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

A. The facility declares an emergency or is responding to a natural disaster that makes the management of client information security secondary to immediate personnel safety activities.
B. Management determines that granting immediate access is in the best interest of the client.
C. If management grants emergency access, she/he shall review the impact of

emergency access and document the event within 24 hours of it being granted.

D. 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.

2.3.4.2 Granting Emergency Access to an Existing User Access Account

In some circumstances it may be necessary for management to grant emergency access to a user's account without the user's knowledge or permission.

Management may grant this emergency access in these situations:

A. The workforce member terminates or resigns and management requires access to the person's data;

B. The workforce member is out for a prolonged period;

C. The workforce member has not been in attendance and therefore is assumed to have resigned.; and

D. Manager/supervisor needs immediate access to data on a workforce member's computer in order to provide client treatment.

<u>2.3.5 Termination of Access</u>

The department manager or his/her designated representative is responsible for terminating a workforce member's access to ePHI in these circumstances:

2.3.5.1 If management has evidence or reason to believe that the individual is using information systems or resources in a manner inconsistent with the Security Rule policies.

2.3.5.2 If the workforce member or management has evidence or reason to believe the user's password has been compromised.

2.3.5.3 If the employee resigns, is terminated, is suspended, retires, or is away on unapproved leave.

2.3.5.4 If the employee's job description changes and system access is no longer justified by the new job description.

2.3.5.5 If the workforce member is on an approved 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.

<u>2.3.6 Modifications to the Workforce members Access</u>

2.3.6.1 Transfers within

If a workforce member transfers or changes role within a department the workforce member's new supervisor or manager is responsible for evaluating the member's current access and for requesting new access to ePHI commensurate with the workforce member's new role and responsibilities.

2.3.6.2 Transfers outside

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

A. The workforce member's access to ePHI within his or her current unit shall be terminated as of the date of transfer.

B. The workforce member's new supervisor or manager is responsible for requesting access to ePHI commensurate with the workforce member's new role and responsibilities.

2.3.7 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 covered components:

2.3.7.1 Non use of account

Every new User ID or log-on 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.

2.3.7.2 Periodic reviews

At least every six months, IT teams are required to send supervisors/managers (or appropriate designees) a list of:

A. All workforce members for all applications;
B. Workforce members and their access rights for all shared folders that contain ePHI, and
C. All Virtual Private Network workforce members.

The supervisors/managers shall then notify their IT teams of any workforce members that no longer require access.

The remainder of this policy document left intentionally blank.

2.4 Policy Responsibilities:

2.4.1 Department Security Officer or Designee Responsibilities:

2.4.1.1 Terminate and transfer, regular notice

Work with HR or designee to arrange a regularly occurring email to IT or designee with the names of workforce members who are terminating or transferring out of the covered component, along with the individual's supervisor's name and the effective date.

2.4.1.2 Immediate notice on Termination

Work with HR or designee to arrange a process to immediately email and telephone IT and Facilities Services if a workforce member is being terminated. The HR division shall provide the workforce member's name, supervisor's name and effective date, so that access can be discontinued when the personnel action is effective. Immediately, upon written notification, the worker's access to ePHI shall be removed.

2.4.2 Covered Components' IT Team(s) Responsibilities: Account Management

2.4.2.1 Reports

A. A report shall be created that identifies new User IDs or log on accounts not accessed within 30 days of creation.

B. A report shall be provided every six months to the manager/supervisor or designee documenting workers with access to ePHI, and requesting verification that access is still required to fulfill the worker's job functions.

2.4.3 Managers and Supervisors Responsibilities:

2.4.3.1 Minimum necessary

Each manager/supervisor is responsible for ensuring that the access to ePHI granted to each of his or her subordinates is the minimum necessary access required for each such subordinate's job role and responsibilities.

2.4.3.2 Terminate access

If the user no longer requires access, it is the manager/supervisor's responsibility to complete the necessary paperwork as soon as possible to terminate access.

2.4.3.3 Validate access

The manager/supervisor shall validate new User IDs or log on accounts that are not accessed within 30 days of creation. If access is no longer required, the User ID shall be deleted.

2.4.3.4 Verify information on reports

Semi-annual user and folder access reports and the VPN access reports prepared by the IT team shall be reviewed and verified to determine if the workforce members still require access to the ePHI.

2.4.3.5 Agreement and training

The manager/supervisor shall ensure members of the workforce have signed the Employee Acknowledgement Form and are properly trained before approving access to ePHI.

2.4.4 User Responsibility:

Each user shall read and sign the Employee Acknowledgement Form, attend HIPAA Security training, and report all security incidents.

2.5 Procedures

Each covered component shall document written procedures for granting user access, the authorization of access to ePHI, and the termination of user access. These procedures shall include as a minimum all of the policy requirements above.

Each covered component shall submit all new and revised procedures to the County Administrative Office for approval and ongoing evaluation. Any procedures developed by covered components shall be consistent with the County HIPAA policies and not deviate from the County standard.

The remainder of this policy document left intentionally blank.

Policy 3: Authentication & Password Management

3.1 HIPAA Regulation:

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

3.2 Policy Purpose:

Passwords are an important aspect of computer security and are the front line of protection for user accounts. A compromised password may, in turn, result in a security breach of the County's network. All County workforce members are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. The purpose of this policy is to reinforce the use of effective passwords, also known as strong passwords, and require workforce members to change their passwords on a regular basis. This policy applies only to information systems that contain or have access to ePHI.

3.3 Policy Description:

Information systems used to access ePHI shall uniquely identify and authenticate workforce members.

<u>3.3.1 Authentication - Verification</u>

Industry standard authentication protocols shall be configured on all routers and switches used in the Wide Area Network (WAN) and the local area networks (LANs). Authentication types can include:

Unique user ID and passwords
Biometrics identification system
Telephone callback
Token system that uses a physical device for user identification
Two forms of authentication for wireless remote access

Information systems used to access ePHI shall identify and authenticate connections to specific devices involved in system communications (digital certificate, for example)

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

<u>3.3.2 Unique User ID and Password Management</u>

All County workforce members are assigned a unique user ID to access the network. All workforce members are responsible for creating and maintaining the confidentiality of the password associated with their unique user ID. Managers/supervisors are required to ensure that their staff understands the user responsibilities for securely managing confidential passwords.

Upon receipt of a user ID, the person assigned the user ID is required to change the password provided by the administrator to a password that only he or she knows. Effective passwords shall be created in order to secure access to electronic protected health information (ePHI).

Workforce members who suspect that their password has become known by another person shall change their password immediately. No user shall give his or her password to another person.

Workforce members are required to change their network user ID passwords every six months; when the technology is capable, each application access password shall be changed every six months. Where technology is capable, network and application systems shall be configured to enforce automatic expiration of passwords every six months.

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

All passwords are to be treated as sensitive, confidential Plumas County information. If managers/supervisors require emergency access to a worker's email or individual network drive, see the emergency access section of the County's HIPAA User Access Management policy.

NOTE: There are some applications that do not have the capability to require a unique user ID or unique passwords. These applications are being replaced and eventually shall be legacy systems used for researching historical data. Sharing passwords in these applications is allowed until the applications are replaced. No new applications that contain electronic protected health information (ePHI) are allowed to be implemented that do not have the capability to assign unique user ID and associated confidential passwords.

3.3.3 User ID & Password Guidelines

Where possible, implement unique user IDs that are different from the e-mail address; covered components are encouraged not to use standard naming conventions for user IDs and should avoid using the same email user name as the system user ID.

Strong password requirements when technology is capable include:
1 Using passwords that are not found in the dictionary
2 Using passwords with six to eight characters or more; or pass phrases if allowed
3 Starting and ending with a letter or symbol with special characters included between letters can be either upper or lower case, but shall always be entered in the same case
4 Containing at least one number between the first and last character
5 Containing at least one allowable symbol anywhere in the sequence
6 Always being significantly different from prior passwords.
7 Never containing the user's name or any part of the user's full name
8 Never selecting a password the user needs to write down to remember

Password protection requirements for users:
1 Never reveal a password over the phone to anyone
2 Never reveal a password in an email message
3 Never reveal a password to your supervisor
4 Never talk about a password in front of others
5 Never hint at the format of a password (e.g., "my family name")
6 Never reveal a password on questionnaires or security forms

7 Never share a password with family members
8 Never reveal a password to co-workers
9 Never use words such as “password”, “secure”, “secret”, “confidential”, “restricted”, or “private” as your password
10 Never write down your password; instead memorize it
11 Never use the same password for Plumas County user access and other non-Plumas County access (e.g., personal ISP account, option trading, benefits, etc.)
12 Never keep a list of user ID’s and passwords in your office
13 Never misrepresent yourself by using another person’s user ID and password.

3.4 Policy Responsibilities:

3.4.1 Managers and Supervisors Responsibility

Managers/supervisors are responsible to reinforce secure password use in their offices with emphasis on “no password sharing”. If access to another worker’s account is required, managers/supervisors shall follow the emergency access section of the County’s HIPAA User Access Management policy.

3.4.2 IT Team(s) Responsibilities for Network User ID Creation

System administrators shall provide the password for a new unique user ID to only the user to whom the new ID is assigned.

Workforce members may at times request that their password be reset. System administrators shall verify the identity of the user requesting a password reset or verify that the person making the request is authorized to request a password reset for another user. When technically possible, a new or reset password shall be set to expire on its initial use at log on so that the user is required to change the provided password to one only they know.

3.4.3 All Workforce members accessing ePHI

Any workforce member who suspects that their password has become known by another person shall change their password immediately.

3.5 Procedures

Each covered component shall create and implement procedures that are consistent with County policies.
Each covered component shall submit all new and revised procedures to the County Administrative County Administrative Office for approval and ongoing evaluation. Any procedures developed by covered components shall be consistent with the County HIPAA policies and not deviate from the County standard.

The remainder of this policy document left intentionally blank.

Policy 4: Facility Access Controls

4.1 HIPAA Regulation:

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

4.2 Policy Purpose:

The intent of this policy is to establish protocols for securing facilities that contain EPHI.

4.3 Policy Description:

4.3.1 General

The County of Plumas 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.

4.3.2 New or Remodeled Facility in a covered component

When changing an existing facility or moving into a different facility department heads shall ensure the facility plan components below are compliant with the HIPAA Regulations.

4.3.3 Facility Security Plan

The County shall safeguard the facilities of its covered components and the equipment therein from unauthorized physical access, tampering, and theft. The department head in coordination with the Department Security Officer (DSO) shall annually audit covered component facilities to ensure EPHI safeguards are continuously being maintained.

4.3.3.1 Facility security guidelines for the workforce

A. Do not share access cards to enter the facility;
B. Do not allow other persons to enter the facility by “piggy backing” *(entering the facility by walking behind an authorized person through a door without using a card in the reader);*
C. Do not share hard key access to enter the facility; and
D. Do not share alarm codes or keypad codes to enter the facility

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

4.3.3.2 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 facilities structure, the type of visitors, and where the ePHI is accessible.

4.3.3.3 Security Access Cards

Some facilities have security access key cards (*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 cards. When administering security access cards each 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 persons leave County employment or discontinue volunteer service;
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 cards inactive for 90 days or more to determine if the access card shall be disabled; and
H. A tracking mechanism to identify all workforce members with security card access in each facility.

4.3.3.4 Keypads/Cipher Locks

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

A. Clearances based on programmatic need, special mandated security requirements and workforce member security, and
B. A mechanism to track which workforce members are provided access.

4.3.3.5 Metal/Hard Keys

Facilities that use metal/hard keys shall change affected or appropriate key locks when keys are lost or a workforce member leaves without returning the key. In addition, the facility shall have:

A. Clearances based on programmatic need, special mandated security requirements and workforce member security; and
B. A mechanism to track which workforce members are provided access.

4.3.3.6 Network Closet(s)

Every network closet shall be locked whenever the room is unoccupied or not in use. Covered components shall document who has access to the network closets and periodically change the locking mechanism to these closets.

4.3.3.7 Server Room(s)

Every server room shall be locked whenever the room is unoccupied or not in use. Covered components shall document who has access to each server room and periodically change the locking mechanism to server rooms.

4.3.3.8 Alarm Systems

When feasible buildings that have 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 that require this information in order to leave and enter a building. These alarm codes shall be changed at least every six months.

4.3.3.9 Doors

All external facility doors and doors to areas with ePHI shall remain completely shut 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. Sometimes the doors do not completely close by themselves. 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.

4.3.4 Contingency Operations - Emergency Access to Facilities

Each facility shall have emergency access procedures in place that allow facility access to appropriate persons to access data as well as support restoration of lost data. 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.

4.3.5 Maintenance Records Policy

The County Facilities Services Director will notify department directors of all facility modifications that potentially effect security prior to any modification. Repairs or modifications to the physical building for each facility where ePHI can be accessed shall be logged and tracked when such repairs potentially impact security procedures. These repairs will be logged by individual department heads in a Quality Assurance Security Log. The log shall include events that are related to security (for example, repairs or modifications of hardware, walls, doors, and locks).

4.4 Policy Responsibilities:

4.4.1 Manager/supervisor Requirements:

4.4.1.1 Corrective actions

Take appropriate corrective action against any person who knowingly violates the facility plan;

4.4.1.2 Authorize

Authorize clearances that are appropriate to the duties of each workforce member;

4.4.1.3 Notifications

Notify the security administrator or designee within one business day when a user no longer requires access to the facility; and

4.4.1.4 Verify surrenders

Verify that each worker surrenders her/his card or key upon leaving employment.

4.4.2 Worker Requirements:

4.4.2.1 Display access card

Display their access/security card to demonstrate their authorization to access restricted areas;

4.4.2.2 Report lost/stolen access card

Immediately report lost or stolen cards, or metal keys or keypad-cipher lock combinations;

4.4.2.3 Surrender access card

Surrender access card or key upon leaving employment

4.4.3 Facility Manager/Department Security Officer or Designee Requirements:

4.4.3.1. Responsible for repairs

Request and track maintenance repairs;

4.4.3.2 Emergency access

Establish and maintain a mechanism for accessing the facility in an emergency;

4.4.3.3. Track access

Track who has access to the facility;

4.4.3.4. Change access mechanisms

A. Change metal locks when a key is lost or unaccounted for;
B. Change combination keypads/cipher locks every three months;
C. Change the alarm code every six months;
D. Disable access cards not used for 90 days or more;

4.4.3.5 Audits

Complete access card audits every 6 months to verify user access

4.4.4), County Administrative Officer Information Technology Director (ITD Requirements:

4.4.4.1 Ensure compliance

Work with covered components to ensure facilities comply with the HIPAA Security Rule for facility access controls; and

4.4.4.2 Audits

Conduct annual audits of covered component facilities to ensure the facility is secured and the requirements of this policy are being enforced.

4.5 Procedures:

Each covered component shall document written procedures for their facility security plan. Procedures shall be written to address the unique requirements of each facility. An essential part of compliance is to document and implement processes to ensure the safeguards in the facility security plan are being maintained.

Each covered component shall submit new and revised procedures and plans to the County Administrative Office for approval and ongoing evaluation. Any procedures developed by covered components shall be consistent with the County HIPAA policies and not deviate from the County standard.

The remainder of this policy document left intentionally blank.

Policy 5: Workstation Access Controls

5.1 HIPAA Regulation:

Access control and validation procedures
Workstation use
Workstation security
Automatic log off

5.2 Policy Purpose:

The intent of this policy is to establish rules for securing workstations that access ePHI. Since ePHI is portable, this policy requires workforce members to protect ePHI in all locations, including, but not limited to, homes or client sites.

5.3 Policy Description:

5.3.1 General

The County of Plumas shall reasonably safeguard electronic protected health information (ePHI) from any intentional or unintentional use or disclosure.

5.3.2 Workstation Use: Security

The County of Plumas workforce members shall ensure that observable confidential information is adequately shielded from unauthorized disclosure and unauthorized access on computer screens. Each County of Plumas workplace shall make every effort 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 covered components shall be aware of their surroundings to ensure no one can incidentally view ePHI and no ePHI is left unattended.

Workforce members who work from home or other non office sites shall take the necessary steps to protect ePHI from other persons who may have access to their home or other non office site. This includes password protection of their personal computers, and security for all other forms of portable ePHI such as locking up CD ROM Disks, floppy disks, USB drives, PDAs, and laptops.

User session-lock shall be implemented when the computer is left idle. It shall be automatic after a specific time based on location and function. The session shall be locked to disable access to the PC until the user enters their unique authenticator.

When technology is capable, while accessing ePHI outside the Plumas County Wide Area Network (for example: extranet, VPN) automatic log off shall occur after a maximum of 30 minutes of inactivity. Automatic log off is a system enabled enforcement of session termination after a period of inactivity and blocks further access until the workforce member reestablishes the connection using the identification and authentication process.

5.4 Policy Responsibilities:

5.4.1 Manager/supervisor requirements:

5.4.1.1 Corrective actions

Take appropriate corrective action against any person who knowingly violates the security of workstation use;

5.4.1.2 Ensure lock outs

Ensure that workers set their computer to automatically lock when the computer is not in use; and

5.4.1.3 Ensure controlled access

Ensure that all confidential information is not viewable by unauthorized persons at workstations in offices under their management.

5.4.2 Worker Requirements:

5.4.2.1 Computer lock out

Ensure the computer is set to automatically lock the session when the computer is not in use;

5.4.2.2 Control access

Ensure that all confidential information is not viewable by unauthorized persons; and when working from home or other non-office work sites, protect ePHI from unauthorized access or viewing.

5.4.3 IT Support:

5.4.3.1 Computer lock out and log off

When installing new workstations, set the session lock timer to lock the computer when left unattended; and when installing new systems or applications, set the automatic logoff timer to terminate the session when the computer is left unattended.

5.5 Procedures:

Workforce members shall utilize these procedures for protecting workstations:

Use of polarized screens or other computer security screen overlay devices that shield confidential information;

Placement of computers out of the visual range of persons other than the authorized user;

Clearing confidential information from the screen when it is not actively in use;

Setting an automatic session lock option on all computer workstations;

Shutting down or locking workstation sessions when left unattended; and

When the technology is capable, setting the applications to automatically log off after a specific time of inactivity.

Each covered component shall develop and implement procedures. Covered components shall submit all new and revised procedures to the County Administrative Office for approval and ongoing evaluation. Any procedures developed by covered components shall be consistent with the County HIPAA policies and not deviate from the County standard.

The remainder of this policy document left intentionally blank.

Policy 6: Device & Media Controls

6.1 HIPAA Regulation:

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

6.2 Policy Purpose:

The intent of this policy is to ensure that ePHI stored or transported on storage devices and removable media is appropriately controlled and managed.

6.3 Policy Description:

6.3.1 Device and Media Controls/ Accountability

Each covered component shall protect all the hardware and electronic media that contain electronic protected health information (ePHI). This includes, but is not limited to, personal computers, PDAs, laptops, storage systems, backup tapes, CD Rom disks, and removable disks.

Each covered component is responsible to develop procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility. Procedures shall include maintaining a record of movements of hardware and electronic media and any person responsible therefore.

6.3.2 Portable Media Use - Security

In addition to protecting County's workstations and facilities, workforce members shall protect ePHI when working from all other locations, including home, other county offices, or when working in the field.

In order to limit the amount of portable ePHI, workforce members shall not save quantities of ePHI on floppy disks, CD ROM Disks and other portable items when it is not necessary for the performance of their assignment.

In addition, no portable ePHI shall be the original and only source of the data. This information shall be stored either on the network or an electronic media that can be retrieved in an emergency.

Methods for protecting portable media with ePHI include:

6.3.2.1 Permission required for removal

All workforce members shall receive permission from their supervisor before removing ePHI from their facility. The level of permission is determined by the covered component. Approvals shall include the type of permission and the time period for authorization. The time period shall be a maximum of one year.

6.3.2.2 EPHI at locations other than facility

Workforce members who work in the field shall not to leave ePHI unlocked or visible in their vehicles or leave any ePHI in client facilities/homes.

6.3.2.3 Lost EPHI

If ePHI is lost, workforce members are responsible to promptly contact their supervisor, the department's Security Officer (SO) or designee and the County Administrative County Administrative Office within one business day upon awareness that ePHI is lost.

6.3.3 Disposal

Before electronic media that contains ePHI can be disposed, the following actions shall be taken on computers used in the workplace, at home, or at remote sites:

6.3.3.1 **Hard drives** shall be either wiped clean or destroyed. Hard drive cleaning shall meet the Department of Defense (DOD) standards, which states *"the method of destruction shall preclude recognition or reconstruction of the classified information or material."* In addition, the hard drive shall be tested to ensure the information cannot be retrieved.

6.3.3.2 **Backup tapes** shall be destroyed or returned to the owner and their return documented. Destruction shall include a method to ensure there is no ability to reconstruct the data.

6.3.3.3 **Other media**, such as memory sticks, USB flash drives or micro drives, CD-ROMs and floppy disks, shall be physically destroyed (broken into pieces) before disposing of the item.

6.3.4 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 or when the equipment is transferred to a new worker with different ePHI access needs. Hard drives shall be wiped clean before transfer. Cleaning shall meet the Department of Defense (DOD) standards which states *"the method of destruction shall preclude recognition or reconstruction of the classified information or material."* In addition, the hard drive shall be tested to ensure the information cannot be retrieved.

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.

6.3.5 Sending a Computer Server Hard Drive to Repair

When the technology is capable, an exact copy of the ePHI shall be created and the ePHI removed from the server hard drive before sending the device out for repair.

6.3.6 Moving Computer Server Equipment with ePHI

Before moving server equipment that contains ePHI, a retrievable exact copy needs to be created.

6.3.7 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.)

6.4 Policy Responsibilities:

6.4.1 Manager/supervisor responsibilities:

Ensure that only workforce members who require the need to remove ePHI from their facilities are granted permission to do so.

6.4.2 IT Responsibilities

Ensure all hard drives are wiped clean before disposal or reuse;
Test hard drives to ensure they are clean;
Before moving hardware or sending hard drives for repair that contains ePHI, create a retrievable copy of the data; and
Maintain an inventory and a record of movements of hardware and electronic media such as workstations, servers, or backup tapes.

6.4.3 Workforce Responsibilities:

Laptops, PDAs, CD ROM Disks, and floppy disks, and other portable media that contain EPHI shall be tracked by individual workforce members or their units. To limit the amount of portable EPHI, workforce members shall not save quantities of ePHI onto floppy disks, CD-ROMs and other portable items when it is not necessary. Workforce members shall remove and destroy all EPHI before disposing the media.

6.5 Procedures

Each covered component shall document written procedures to track, dispose, and reuse media devices used for ePHI.

Each covered component shall submit all new and revised procedures to the County Administrative Office for approval and ongoing evaluation. Any procedures developed by covered components shall be consistent with the County HIPAA policies and not deviate from the County standard.

The remainder of this policy document left intentionally blank.

PLUMAS COUNTY
HIPAA SECURITY POLICY

Policy 7: Audit Controls

7.1 HIPAA Regulation:

Log-in monitoring
Information system activity review
Audit controls

7.2 Policy Purpose:

The intent of this policy is to provide the authority for workforce members representing the County IT organizations and specified contractors to conduct a security audit on County computing resources.

Activity reviews provide indications that implemented safeguards are working, or that safeguards are insufficient. Audits may be conducted to:

1 Ensure integrity, confidentiality, and availability of information and resources
2 Investigate possible security incidents to ensure conformance to County of Plumas security policies.
3 Monitor user or system activity where appropriate
4 Verify that software patching is being maintained at the appropriate security level
5 Verify virus protection is being maintained at current levels

7.3 Policy Description:

7.3.1 Log-in Monitoring

The County has the right to monitor system access and activity of all workforce members.

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

7.3.1.1 Monitor log in attempts

A mechanism to log and document four or more failed log-in attempts in a row shall be implemented on each network system containing ePHI when the technology is capable.

7.3.1.2 Review of logs

Log-in activity reports and logs shall be reviewed monthly at a minimum to identify any patterns of suspicious activity.

7.3.1.3 Report of failed log ins

All failed log-in attempts of a suspicious nature, such as continuous attempts, shall be reported immediately to the Information Security Officer (ISO) or the designee for each covered component.

7.3.1.4 Disable user ID

To the extent that technology allows, any user ID that has more than four repeated failed log-in attempts in a row shall be disabled for a minimum of 30 minutes.

7.3.2 Information System Activity Review – Audit Controls

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

7.3.2.1 Log events

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.

7.3.2.2 Quarterly review of logs

Each fiscal quarter, at a minimum, every application and system administrator or designee shall review audit logs, activity reports, or other mechanisms to document and manage system activity.

7.3.2.3 Report misuse

Indications of improper use shall be reported to management for investigation and follow up.

7.3.2.4 Archive logs

Audit logs of access to networks and applications with ePHI shall be archived.

7.3.2.5 Protect audit information

Audit information and audit tools shall be protected from unauthorized access, modification, and deletion.

7.4 Policy Responsibilities:

Directors, IT Director and the County Administrative Officer are responsible to implement and monitor audit controls for all systems that contain ePHI.

7.5 Procedures

Each covered component shall submit all new and revised procedures to the County Administrative Office for approval and ongoing evaluation. The County Administrative Office shall create audit control checklists and logs to assist with, and standardize, the audit function. Any procedures developed by covered components shall be consistent with the County HIPAA policies and not deviate from the County standard.

The remainder of this policy document left intentionally blank.

Policy 8: Security Incident – Response & Reporting

8.1 HIPAA Regulation:

Security incident procedures
Response and reporting

8.2 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. It is imperative that a formal reporting and response policy be followed when responding to security incidents.

8.3 Policy Description:

The County shall employ tools and techniques to monitor events, detect attacks, and provide identification of unauthorized use of the systems that contain ePHI.

8.3.1 Reporting

All security incidents, threats, or violations that affect or may affect 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 Virus, worm, or other malicious code attacks
2 Network or system intrusions
3 Persistent intrusion attempts from a particular entity
4 Unauthorized access to ePHI, an ePHI based system, or an ePHI based network
5 ePHI data loss due to disaster, failure, error, theft
6 Loss of any electronic media that contains ePHI
7 Loss of the integrity of ePHI
8 Unauthorized person found in a covered component's facility

Individual county department heads and Department Security Officers shall be notified immediately of any suspected or real security incident. If it is unclear as to whether a situation is a security incident, the IT Department or contracted IT resource shall be contacted to evaluate the situation.

8.3.2 Response and Resolution

The IT Department or contracted IT resource shall report the incident to the covered component's the Department Head. The Department Head shall determine if a report of the incident shall be forwarded to the County Administrative Office. The IT Department shall resolve the incident when possible. The Department Head shall evaluate the report to determine if an investigation of the incident is necessary. The Department Head in consultation with the CAO shall determine if County Counsel, law enforcement or Human Resources are to be contacted regarding the incident.

8.3.3 Logging

All HIPAA security related incidents and their outcomes shall be logged and documented by the IT Department. Individual Department Heads will document and log incidents and outcomes.

The County shall train personnel in their incident response roles and responsibilities and provide refresher training as needed. The County shall test the incident response capability at least annually using tests and exercises to determine the effectiveness.

8.4 Policy Responsibilities:

8.4.1 Workforce members

Workforce members are responsible to promptly report any security related incidents to their respective Department Heads. Department Heads will report incidents to the IT Department.

8.4.2 IT Department

The IT Department documents all security incidents.

8.4.3 County Administrative Office , County Privacy Officer, ISO, and CISO

The Department Director in consultation with County Administrative Officer will determine if the incident requires further investigation as well any corrective action to be taken. The County Administrative Office is responsible for maintaining all documentation on security breaches for six years.

8.5 Procedures:

Each covered component shall submit all new and revised procedures to the County Administrative Office for approval and ongoing evaluation. Any procedures developed by covered components shall be consistent with the County HIPAA policies and not deviate from the County standard.

The remainder of this policy document left intentionally blank.

Policy 9: Transmission Security

9.1 HIPAA Regulation:

Transmission security
Integrity controls
Encryption and decryption
Encryption

9.2 Policy Purpose:

The intent 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.

9.3 Policy Description:

9.3.1 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 Technology Director.

9.3.1.1 Encryption Required:

A. No ePHI shall be sent outside the County countyofplumas.com domain unless it is encrypted. This includes all email and email attachments sent over a public internet; and

B. When accessing a secure network an encryption communication method, such as VPN, shall be used.

9.3.1.2 Encryption Optional:

A. When using a private circuit (point to point) to transmit ePHI, no encryption is required; and

B. Dialup connections directly into secure networks are considered to be secure connections for ePHI and no encryption is required.

9.3.2 Transmission and Modem Use:

9.3.2.1 Modems shall never be left connected to personal computers in auto-answer mode.

9.3.2.2 Dialing directly in to or out of a desktop computer that is simultaneously connected to a local area network or another internal communication network is prohibited. Dial-up access to WAN connected personal computers at the office is prohibited.

9.3.4 EPHI Transmissions Using Wireless LANs and Devices within the Plumas

County domain

9.3.4.1. The transmission of ePHI over a wireless network within the countyofplumas.com domain is permitted if both of the following conditions are met:

A. The local wireless network is utilizing an authentication mechanism to ensure that wireless devices connecting to the wireless network are authorized;

B. The local wireless network is utilizing an encryption mechanism for all transmissions over the aforementioned wireless network and uses two types of authentication B) If transmitting ePHI over a wireless network that is not utilizing an authentication and encryption mechanism, the PHI shall be encrypted before transmission.

9.3.5 Perimeter Security

Any external connection to the Plumas County Wide Area Network (WAN) shall come through the perimeter security's managed point of entry. If determined safe by the IT Director, outbound services shall be initiated for internal addresses to external addresses. Inbound services shall be negotiated on a case by case basis with the IT Director. All workforce members connecting to the WAN shall sign the Employee Acknowledgement Form before connectivity is established.

9.3.6 Firewall Controls to transmit EPHI into and out of Plumas County

Networks containing systems and applications with EPHI shall implement perimeter security and access control with a firewall. Firewalls shall be configured to support the following minimum requirements:

9.3.6.1 Limit access

Limit network access to only authorized workforce members and entities; Limit network access to only legitimate or established connections (*An established connection is return-traffic in response to an application request submitted from within the secure network.); and*

9.3.6.2 secure and disable

Console and other management ports shall be appropriately secured or disabled

9.3.6.3 The configuration of firewalls used to protect networks containing ePHI-based systems and applications shall be submitted to the Perimeter Security Team for review and approval.

9.4 Policy Responsibilities:

All workforce members that transmit ePHI outside the County WAN are responsible for ensuring the information is safeguarded by using encryption when using the public internet or a wireless device.

The IT Director is responsible for the perimeter security architecture, its resources, its periodic auditing, and testing.

9.5 Procedures:

Each covered component shall submit all new and revised procedures to the County Administrative Office for approval and ongoing evaluation. Any procedures developed by covered components shall be consistent with the County HIPAA policies and not deviate from the County standard.

The remainder of this policy document left intentionally blank.

Policy 10: Protection from Malicious Software

10.1 HIPAA Regulation:

- *Protection from malicious software*

10.2 Policy Purpose:

The intent 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, and trojans.

10.3 Policy Description:

The County of Plumas' covered components shall ensure all computers (owned, leased, and/or operated by the covered components) install and maintain anti-virus software. All workstations shall be configured to activate and update anti-virus software automatically each time the computer is turned on or the user logs on the network.

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

10.4 Responsibilities

10.4.1 Workforce Responsibilities:

10.4.1.1 Workforce members who utilize laptops to log on to the network shall work with their IT support to ensure all updates are received.

10.4.1.2 Workforce members are not to disable automatic virus scanning features.

10.4.1.3 All non-county computers that directly access the WAN shall have anti-virus software and remain current with updates.

10.4.1.4 All downloaded files shall be virus-checked prior to use.

10.4.1.5 All storage media (i.e. disks) shall be treated as if they contain viruses. Workforce members are permitted to use removable storage disks provided that all disks are virus checked prior to use.

10.4.1.6 If a virus is detected, workforce members are instructed to immediately contact their IT Department.

10.4.1.7 For the purposes of protecting data and preventing the spread of viruses, workers shall:

E. Attend HIPAA security training which includes virus protection issues and current malicious software trends;

F. Maintain back up copies of data files

10.4.2 IT Responsibility:

Set up laptop computers so they automatically load virus updates when they are connected to the County network.

10.5 Procedures

To ensure that all Plumas County workforce members are made aware of the threats and vulnerabilities due to malicious code and software such as viruses and worms and are effectively trained to identify and prevent these types of attacks, the following procedures shall be established and implemented:

10.5.1. The workforce is trained to identify and protect data, when possible, against malicious code and software.

10.5.2. Security reminders are given to the workforce to inform them of any of new virus, worm, or other type of malicious code that may be a threat to ePHI.

Each covered component shall submit all new and revised procedures to the County Administrative Office for approval and ongoing evaluation. Any procedures developed by covered components shall be consistent with the County HIPAA policies and not deviate from the County standard.

The remainder of this policy document left intentionally blank.

Policy 11: Contingency Plan

11.1 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

11.2 Policy Purpose:

The purpose of this policy is to establish rules for continuing business without the normal resources of the organization.

11.3 Policy Description:

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

. Applications and data criticality analysis
Data backup
. Disaster Recovery Plan
. Emergency mode operation plan

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

11.3.1 Applications and Data Criticality Analysis

11.3.1.1 Each HIPAA covered component shall assess the relative criticality of specific applications and data within the covered component for purposes of developing its Data Backup Plan, its Disaster Recovery Plan and its Emergency Mode Operation Plan.

11.3.1.2 Each covered component shall Identify critical business functions, define impact scenarios, and determine resources need to recover from each impact.

11.3.1.3 The assessment of data and application criticality shall be conducted periodically and at least annually to ensure that appropriate procedures are in place for data and applications at each level of risk.

11.3.2 Data Backup Plan

11.3.2.1 All ePHI shall be stored on network servers in order for it to be automatically backed up by the system.

11.3.2.2 ePHI shall not be saved on the local drives of personal computers.

11.3.2.3 EPHI stored on portable media shall be saved to the network to ensure backup of ePHI data.

11.3.2.4 The County shall conduct daily backups of user-level and system-level information and store the backup information in a secure location. A weekly backup shall be stored offsite.

11.3.2.5 Each covered component shall establish and implement a Data Backup Plan pursuant to which it would create and maintain retrievable exact copies of all ePHI.

11.3.2.6 The Data Backup Plan shall apply to all files that may contain ePHI.

11.3.2.7 The Data Backup Plan shall require that all media used for backing up ePHI be stored in a physically secure environment, such as a secure, off-site storage facility or, if backup media remains on site, in a physically secure location, different from the location of the computer systems it backed up.

11.3.2.8 If a non-County off-site storage facility or backup service is used, a written contract shall be used to ensure that the contractor shall safeguard the ePHI in an appropriate manner.

11.3.2.9 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.

11.3.2.10 Each covered component shall submit its new and revised Data Backup Plan to the County Administrative Office for approval.

11.3.3 Disaster Recovery Plan

11.3.3.1 To ensure that each covered component can recover from the loss of data due to an emergency or disaster such as fire, vandalism, terrorism, system failure, or natural disaster effecting systems containing ePHI, each covered component shall establish and implement a Disaster Recover Plan pursuant to which it can restore or recover any loss of ePHI and the systems needed to make that ePHI available in a timely manner. The Disaster Recovery Plan for each covered component shall be incorporated into the Countywide Disaster Recovery Plan.

11.3.3.2 The Disaster Recovery Plan shall include procedures to restore ePHI from data backups in the case of a disaster causing data loss.

11.3.3.3 The Disaster Recovery Plan shall include procedures to log system outages, failures, and data loss to critical systems, and procedures to train the appropriate personnel to implement the disaster recovery plan.

11.3.3.4 The Disaster Recovery Plan shall be documented and easily available to the necessary personnel at all time, who shall be trained to implement the Disaster Recovery Plan.

11.3.3.5 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.

11.3.3.6 Each covered component shall submit its new and revised Disaster Recovery Plan to the County Administrative Office for approval.

11.3.4 Emergency Mode Operation Plan

11.3.4.1 Each covered component shall establish and implement (as needed) procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode. Emergency mode operation involves those critical business processes that shall occur to protect the security of electronic protected health information during and immediately after a crisis situation;

11.3.4.2 Emergency mode operation procedures outlined in the Emergency Mode Operation Plan shall be tested on a periodic basis to ensure that critical business processes can continue in a satisfactory manner while operating in emergency mode; and

11.3.4.3 Each covered component shall maintain its Emergency Mode Operation Plan within their respective facilities.

11.4 Policy Responsibilities:

The County Administrative Office shall assure the creation, evaluation, testing, and update of the various contingency plans described herein.

Each covered component shall submit its new and/or revised procedures and plans to the County Administrative Office for approval and ongoing evaluation. Any procedures developed by covered components shall be consistent with the County HIPAA policies and not deviate from the County standard.

The remainder of this policy document left intentionally blank.

Policy 12: Business Associate

12.1 HIPAA Regulation:

Business associate contracts and other arrangements
Written contract or other arrangements

12.2 Policy Purpose:

To document the policy and procedure for determining which contractual and business relationships are considered "Business Associates" as defined by HIPAA. In addition, this policy addresses tracking designated Business Associates and how to follow up on complaints about the Business Associates.

12.3 Policy Description:

12.3.1 Business Associates

The County of Plumas has many contractual and business relationships, and has policies related to its contracts and business relationships. However, not all contractors or business partners are "Business Associates" as defined by HIPAA. This policy only applies to contractors or business partners that come within the definition of a "Business Associate."

Contract managers and County Counsel review contracts to determine if the contract requires a Business Associate agreement. If a Business Associate agreement is required; contract managers complete the Business Associate boiler plate and notify the County Administrative Office. This boiler plate requires the Business Associate to provide satisfactory assurance that the Business Associate shall appropriately safeguard the confidential information and report any security incidents.

12.3.2 Business Associate Non-compliance

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

If such steps are unsuccessful, County of Plumas shall terminate the contract or arrangement, if feasible. If termination is not feasible, the problem shall be reported to the Office of Civil Rights (OCR) within 190 days of the incident.

12.4 Policy Responsibilities:

Contract Managers, County Counsel, and the County Administrative Office shall work together to ensure all Business Associates are identified, tracked and investigated when an allegation is made.

12.5 Procedure:

12.5.1 Tracking and Identifying County of Plumas' Business Associates

The County shall identify those business relationships that meet the definition of a Business Associate. County Counsel shall assure that the appropriate contractual protections are include in all current and new contracts.

12.5.2 Response to Complaints about Business Associates

County workforce members who receive a report or complaint from any source about inappropriate safeguards to ePHI by Business Associates shall provide information regarding that report or complaint to the County Administrative Office. The County Administrative Office shall coordinate with the Business Associate's contract administrator to document the alleged violation and determine if remediation is required in order for the Business Associate to attain contract compliance.

Where contract compliance cannot be attained, the County shall terminate the contract, if feasible. If termination is not feasible, the County Administrative Office shall report the problem to the Office of Civil Rights within 190 days of the incident.

County Counsel shall be contacted and consulted in the event of non-compliance with HIPAA Business Associate provisions.

The remainder of this policy document left intentionally blank.

Policy 13: Monitoring Effectiveness and Assurance

13.1 HIPAA Regulation:

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

13.2 Policy Purpose:

The intent of this policy is to establish periodic evaluations on whether the County is complying with the HIPAA policies and procedures to effectively provide confidentiality, integrity and availability of electronic protected health information (ePHI). Security assessments shall be conducted periodically to determine continued compliance with security standards and specifications. Assessments are conducted to:

13.2.1 Determine if security controls are correctly implemented, and, as implemented, are effective in their application;
13.2.2 Ensure that HIPAA security regulations, policies, and directives are met; and
13.2.3 Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

13.3 Policy Description:

<u>13.3.1 Risk Assessment & Management:</u>

The covered components, shall monitor the effectiveness of their ability to secure ePHI. In order to accomplish this, a risk assessment shall be conducted when:

13.3.1.1 New technology is implemented that either contains ePHI or is used to protect ePHI;
13.3.1.2 New facilities that maintain or house ePHI are designed;
13.3.1.3 Existing facilities that maintain or house ePHI are being remodeled or the design layout is being altered;
13.3.1.4 New programs, functions, or departments are added that affect the security of the County;
13.3.1.5 Security breaches are identified; and
13.3.1.6 Changes in the mode or manner of service delivery are made.

Security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level shall be documented and implemented.

<u>13.3.2 Managing System Changes</u>

The primary goal of managing system changes is to facilitate communications and coordinate all changes that may occur in the IT environment. These changes include, but are not limited to, the installation, update, or removal of network services and components, operating system upgrades, application or database servers and software.

13.3.2.1 Change Notification

A. For informational purposes, the IT Department shall be notified of changes by email no less than 48 hours in advance.

B. Emergency Changes shall be communicated to the IT Department as soon as is reasonable.
C. Any change that encounters difficulties that could adversely affect customers shall be communicated to the IT Department as soon as is reasonable.
D. Customers shall be given notification of all changes (except emergencies) at least 2 business days prior to change.

13.3.2.2 Change Implementation

All non-emergency changes shall occur in a manner that does not disrupt the accessibility and portability of health information.

13.3.2.3 Change Closure

The disposition of all changes shall be documented.

13.3.3 Evaluation

The CAO and IT Director will conduct an assessment of security controls at least annually to determine the extent to which controls are implemented correctly, operating as intended, and producing the desired outcome. Technical and non-technical evaluations are to be conducted periodically to identify any new risks or to determine the effectiveness of the HIPAA Security Policies and Procedures. These evaluations include but are not limited to the following:

1 Random audit reviews of a facility's physical environment security
2 Random audit reviews of workstation security
3 Periodic, unannounced tests of the physical, technical, and administrative controls
4 Assessment of changes in the environment or business process that may affect the HIPAA Security Policies and Procedures.
5 Assessment when new federal, state or local laws and regulations are passed that may affect the HIPAA Security Policies and Procedures
6 Assessment of the effectiveness of the HIPAA Security Policies and Procedures when security violations, breaches or other security incidents occur
7 Assessment of redundancy needed in the network or servers for ePHI availability

13.4 Policy Responsibilities:

13.4.1 County Administrative Office

The County Administrative Office;

1 Is responsible to coordinate with Department Heads and to conduct audits of covered component compliance with the HIPAA security rule
2 Shall coordinate the production of procedures to implement this policy.
3 Is responsible to provide tools and processes for assessing technical and nontechnical evaluations as part of the ongoing compliance efforts.

If assessments recommend changes to the HIPAA Policies and Procedures, the County Administrative Office is responsible to review these changes and present them to management. If needed, the County Administrative Office shall update the workforce training materials.

13.4.2 Department Role

The HIPAA covered component Directors are required to work with their managers/supervisors to ensure technical and non-technical evaluations are being conducted.

Directors shall assure implementation of security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. These measures shall be documented and submitted to the County Administrative Office.

13.5 Procedures:

Departments shall write procedures to ensure ongoing evaluation and assessments are completed to mitigate risks to ePHI. Any procedures developed by covered components shall be consistent with the County HIPAA policies and not deviate from the County standard.

The remainder of this policy document left intentionally blank.

Policy 14: Security Awareness & Training

14.1 HIPAA Regulation:

Security awareness and training
Security reminders

14.2 Policy Purpose:

The intent of this policy is to ensure that all members of the County's workforce that can access electronic protected health information (ePHI), receive the necessary training in order to implement and maintain the HIPAA Security Policies and Procedures and to prevent any violations of confidentiality, integrity or availability of ePHI.

14.3 Policy Description:

14.3.1 Security Awareness Training

Security awareness training is key to eliminating the County's exposure to both malicious threats and accidental errors and omissions.

14.3.1.1 System & Application Training

This policy sets forth a minimum standard for system and application security awareness to reduce the County's risk:

A. Proper uses and disclosures of the ePHI stored in the application;
B. How to properly log on and log off the application;
C. Protocols for correcting user errors;
D. Instructions on contacting a designated person or help desk when ePHI may have been altered or destroyed in error; and
E. Reporting a potential security breach.

14.3.1.2 HIPAA Security Training

All members of the workforce that are part of the covered components shall receive security training. The training and materials are provided by the departments and monitored by County Administrative Office for consistency.

A. Worker Level Training: This training entails security policies and procedures that directly affect workers.
B. Managerial - Supervisory Training: This training entails all the HIPAA Security Policies and Procedures and their role in enforcement and supervision.

All new workforce members are required to attend the appropriate training within 60 days of entering the workforce in a covered component.

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

14.3.2 Tracking Security Training:

Each covered department will assure that its employees receive formal training to assure compliance with the HIPAA Security policy.

Temporary agency workforce members, volunteers, and contracted workers that access ePHI are required to provide the respective department head a copy of a signed training acknowledgment form.

14.3.3 HIPAA Security Reminders

The Department Directors shall develop and implement periodic security updates and issue reminders to the County's workforce. These security reminders shall be provided using any media that is most effective for each covered component (e.g. email, posters, newsletters, intranet site, etc). At a minimum, these reminders shall be provided on a quarterly basis.

14.4 Policy Responsibilities:

Each Department Security Officer (DSO) is responsible for ensuring that all workforce members in their operational areas are trained in the HIPAA security procedures. New workforce members are required to attend department training. A department director may require workforce members to attend more training if security incidents warrant this remedial action.

14.5 Procedures

Each covered component shall document written procedures on how new workers are notified and sent to training.

Each covered component shall submit its new and revised procedures and plans to the County Administrative Office for approval and ongoing evaluation. Any procedures developed by covered components shall be consistent with the County HIPAA policies and not deviate from the County standard.

The remainder of this policy document left intentionally blank.

Policy 15: Sanctions

15.1 HIPAA Regulation:

Sanction policy

15.2 Policy Purpose:

The intent of this policy is to specify enforcement, sanctions, penalties, and disciplinary actions that may be applied against workforce members who fail to comply with the security policies and procedures. This policy ensures that information system workforce members know they can be held accountable for their actions.

15.3 Policy Description:

15.3.1 Sanctions

The definition of the County of Plumas covered entity workforce is taken from the Privacy Rule. In Section 160.103, of the Privacy Rule, the term "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.” The workforce shall guard against improper uses or disclosures of County of Plumas confidential client protected health information.

All members of the County of Plumas covered entity workforce are required to be aware of their responsibilities under County of Plumas HIPAA Security Rule policies.

All members of the County of Plumas covered entity workforce are required to sign the Employee Acknowledgement Form indicating that they have been informed of the business practices in the County of Plumas as it relates to security and privacy.

Managers and supervisors are responsible for assuring that workforce members who have access to ePHI are informed of their responsibilities. Management is responsible for ensuring timely and appropriate training/updates are communicated broadly, and that discontinued information is purged from common usage.

Members of the County of Plumas covered entity workforce who violate County of Plumas policies and procedures regarding the safeguarding of an individual’s confidential information are subject to disciplinary action by County of Plumas 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 Plumas covered entity workforce who knowingly and willfully violate state or federal law for failure to safeguard ePHI are subject to criminal investigation and prosecution or civil monetary penalties.

If County of Plumas fails to enforce security safeguards, the County of Plumas may be subject to administrative penalties by the Office of Civil Rights, including federal funding penalties.

15.3.2 Reporting violations

All workforce members shall notify the Department Security Officer when there is a reasonable belief that any security policies or procedures are being violated.

15.3.3 Retaliation prohibited

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

15.3.3.1 Exercising any right established under County of Plumas policy;

15.3.3.2 Participating in any process established under County of Plumas policy including the filing of a complaint with the County of Plumas or with the Office of Civil Rights;

15.3.3.3 Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing relating to County of Plumas policy and procedures;

15.3.3.4 Opposing any unlawful act or practice, provided that the individual or other person (including a member of the County of Plumas 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 Plumas policy

Those engaging in retaliation shall be subject to the sanctions under this policy.

15.4 Policy Responsibilities:

All workforce members are responsible to notify their Department Security Officer when there is a belief that any security policies are being violated. In addition, suspected violations should be reported to appropriate departmental offices.

The remainder of this policy document left intentionally blank.

Policy 16: Policy Creation and Documentation

16.1 HIPAA Regulation:

Policies and procedures
Documentation
Time limit
Availability
Updates

16.2 Policy Purpose:

The intent of this policy is to formalize the process by which County of Plumas HIPAA Security Rule policies and procedures are created, documented, and implemented in accordance with regulations.

16.3 Policy Description:

16.3.1 Reasonable and Appropriate

The County Administrative Office shall implement reasonable and appropriate County wide policies and procedures to comply with the standards, implementation specifications or other requirements of the HIPAA Security Rule. The County Administrative Office shall work with the following workforce members to draft and revise policies and procedures: respective department heads, IT Director and County Counsel. Department heads shall establish departmental policies as directed by the HIPAA Security Policies and Procedures.

16.3.2 Documented Policies

All policies and procedures implemented to comply with the HIPAA Security Rule shall be documented in writing (which may be in electronic form). All records of actions, activities, or assessments required by the Rule shall be documented. The documentation shall be detailed enough to communicate the security measures taken and to facilitate periodic evaluations.

16.3.2.1 Documentation shall be retained for a minimum of 6 years from the time of its creation or the date when it last was in effect, whichever is later.

16.3.2.2 All documentation shall be available to those persons responsible for implementing the procedures to which the documentation pertains.

16.3.2.3 Documentation shall be reviewed at least annually, and updated as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

16.4 Policy Responsibilities:

16.4.1 County Administrative Office

The County Administrative Office shall be responsible for leading the development, implementation, and maintenance of the policies, procedures, and related documentation.

16.4.2 Department Management

Each covered component shall submit all new and revised procedures to the County Administrative Office for approval and ongoing evaluation.

16.5 Procedures:

In general the following process is used to develop and implement policies and procedures:

16.5.1 New Policies and Updates

The County Administrative Office shall draft new or updated HIPAA information security policies with input and review of the Department Heads, County Counsel, and Human Resources department head, IT Director and as appropriate.

16.5.2 Final Approval of new Policies

The CAO shall give final approval for the new or updated policy.

16.5.3 Communicate new Policies to workforce

The County Administrative Office shall communicate the new or updated policy to the workforce including updating training and related materials as needed.

The remainder of this policy document left intentionally blank.

Appendix A - HIPAA Security Rule / County Policies Crosswalk

HIPAA Security Rule Section		Policy #
Security Management Process	164.308(a)(1)	13
Risk Analysis		13
Risk Management		13
Sanction Policy		15
Information System Activity Review		7
Assigned Security Responsibility	164.308(a)(2)	1
Workforce Security	164.308(a)(3)	2
Authorization and/or Supervision		2
Workforce Clearance Procedure		2
Termination Procedures		2
Information Access Management	164.308(a)(4)	2
Access Authorization		2
Access Establishment and Modification		2
Modification Security Awareness & Training	164.308(a)(5)	14
Security Reminders		14
Protection from Malicious Software		10

Log-in Monitoring		7
Password Management		3
Security Incident Procedures	164.380(a)(6)	8
Response and Reporting		8
Contingency Plan	164.308(a)(7)	11
Data Backup Plan		11
Disaster Recovery Plan		11
Emergency Mode Operation Plan		11
Testing and Revision Procedure		11
Applications and Data Criticality Analysis		11
Evaluation	164.308(a)(8)	13
Business Associate Contracts and Other Arrangements	164.308(b)(1)	12
Written Contract or Other		12
Arrangements Facility Access Controls	164.310(a)(1)	4
Contingency Operations		4
Facility Security Plan		4
Access Control and Validation		4
Procedures Maintenance Records		4
Workstation Use	164.310(b)	5
Workstation Security	164.310(c)	5
Device and Media Controls	164.310(d)(1)	6
Disposal		6

Appendix B – Mapping County Policies to HIPAA Regulations

Policy I: 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: 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). Emergency access procedure. Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

Policy 3: Authentication & 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.
Integrity. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

Policy 4: 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 5: Workstation Access Controls

HIPAA Regulation Covered:

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 6: Device & Media Controls and Disposal

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 7: 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 8: Security Incident – Response & Reporting

HIPAA Regulation Covered:

Security incident procedures. Implement policies and procedures to address security incidents.
Response and Reporting. 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 9: 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. Encryption Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

Policy 10: Protection from Malicious Software

HIPAA Regulation Covered:

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

Policy 11: Contingency Plan

HIPAA Regulation:

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 12: 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 13: Monitoring Effectiveness and Assurance

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 14: Security Awareness & 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 15: Sanctions

HIPAA Regulation:

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

Policy 16: Policy Creation and 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, provided that 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.

Appendix C - Definitions

Terms	Definitions
Business Associate	On behalf of one of the covered components, completes a function or activity involving the use or disclosure of protected health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or, provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.
Covered Component	For the purposes of this policy; each department covered by the HIPAA Security Rule is one covered component –County's covered components include: DHHS, County Counsel, County Executive Office, and Department of Revenue Recovery.
Device	A device is a unit of hardware, outside or inside the case or housing for the essential computer (the processor, memory, and data paths). A device is capable of providing input to the essential computer, receiving output, or both.
Dial Up	Dialing in to a service provider over a modem and phone line
Disposal	The removal or destruction of electronic protected health information from electronic media
Electronic Protected Health Information (EPHI)	**Electronic** Information in electronic format such as - information system applications, internet, intranet, extranet, email, USB drives, computer screens, lap tops, storage devices (magnetic tapes, floppy disks, CDs, optical devices) **Protected Health Information (PHI)** PHI is health information that a covered entity creates or receives that identifies an individual, and relates to: 📬The individual's past, present, or future physical or mental health or condition; 📬The provision of health care to the individual; or 📬The past, present, or future payment for the provision of health care to the individual. **Exceptions: PHI does not include the following:** • Education records •Workman's Compensation records •Health information in workforce member personnel records

Terms	Definitions
Encryption	A method of scrambling or encoding data to prevent unauthorized workforce members from reading or tampering with the data. Only individuals with access to a password or key can decrypt and use the data.
Facility	County owned or leased building in which workers access Electronic Protected Health Information (EPHI)
Firewalls	Special computer programs and hardware that are set up on a network to prevent intruder from stealing or destroying data
Hard Drive	A data storage medium that houses all of the electronic information and software programs on a computer. It is one of the most important pieces of hardware inside a computer.
Hoax	An email that usually states that it is harming the computer, but does not actually perform what it states. Some hoaxes ask the reader of the email to perform a damaging process, like deleting an important file. Most hoaxes are spread by well-meaning individuals hoping to alert others to a potential virus that in reality is just a hoax.
Key Pads – Cipher Locks	Door locks that require a combination entered into in order to unlock the door.
Legacy System	An old or outdated computer system that remains in use even after more modern technology has been installed, usually because a company has invested considerable resources and it holds valuable data
Local Drive	In context to this policy, it is a computer's hard drive (not the network)
Malicious Software	A type of software that includes ways of attacking data integrity, the system itself or the confidentiality of the data. Malicious software includes viruses, virus variants, worms (and superworms) hoaxes, and trojan horses
Media Reuse	A device such as a computer hard drive that contained data that is being reused to contain new data
Modem	A device that translates telephone tones to allow for the multiplexing of data information on the telephone network
Network	A group of computers and associated peripherals connected by a communications channel capable of sharing files and other resources between several workforce members
Network Closets	Concentration of network equipment such as hubs, routers, switches, racks, cables, and sometimes has telephone equipment
Perimeter	Security that protects the network
Portable Media	Usually small devices carried or moved with ease that can contain electronic protected health information such as CD Rom Disks, laptops, USB drives

Terms	Definitions

Private Circuits (PCs)	Well-established digital data circuits. They are point-to-point circuits between two sites providing dedicated capacity. They may be used for voice, video or data traffic or a combination of all of these
Risk Assessment	A process of assessing those factors that could affect confidentiality, availability, and integrity of key information assets and systems. Risk Assessment Authorities are responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets, while minimizing the impact of security procedures and policies upon business productivity.
Security Access Cards	Cards used by the County are called proximity cards (commonly referred to as prox. cards). The credit card-sized card is held up to a reader and acts as an electronic key that unlocks a door. A card's ability to unlock a door is limited by the cardholder's clearance.
Server Room	The room where all the server computers are housed
Strong Passwords	A password that is difficult to detect by both humans and computer programs, effectively protecting data from unauthorized access. A strong password consists of at least six characters that are a combination of letters, numbers and symbols (@, #, $, %, etc.) if allowed. Strong passwords contain the maximum number of characters allowed. Passwords are typically case-sensitive so a strong password contains letters in both uppercase and lowercase. Strong passwords also do not contain words that can be found in a dictionary or any part of the user's own name.
Transmitting	The act of sending a message or data using an electronic medium.
Trojan or Trojan Horse	A trojan or trojan horse is a program generally designed to impact the security of a system. The program is usually disguised as something else (a benign program) or is masqueraded as a legitimate file that the user would expect to see, or want to load, on the system. The payload of a trojan is usually delivered as soon as it is opened and usually with devastating results. Trojans are often used to create "back doors" (a program that allows outside access into a secure network) on computers belonging to a secure network, so that a hacker can have access to the secure network. Trojans are most often delivered as an attachment to a seemingly innocent chain email.
USB drives or USB flash drives	A small, portable flash memory card that plugs into a computer's USB port and functions as a portable hard drive with up to 2GB of storage capacity. USB flash drives are considered easy to use as they are small enough to be carried in a pocket and can plug into any computer with a USB drive.
User	For the purposes of this document, the term user refers to any workforce member (permanent or temporary), contractor, consultant, vendor, volunteer, student or other person who uses, maintains, manages or is otherwise given access privileges to County IT systems.

Terms	**Definitions**

User ID	An identification code which identifies the user to County IT systems
Virtual Private Network (VPN)	A secure, private network connection between two or more devices across the public internet or other shared core network infrastructure. It allows computers at different locations to communicate with each other in a safe and secure environment.
Virus	A program that copies itself into another program, sectors on a drive, or into items that support scripts. Most viruses only copy themselves, while a minority unleash a payload, which is the action generated by the virus. Payloads can damage files, corrupt hard drives, display messages, or open other files. Typically, the payload is delivered when a certain condition occurs, such as when the date on the computer reaches a particular day.
Virus Variant	A virus variant is a virus that has been altered to take advantage of previously created virus code. By doing this, the virus is not immediately detected by anti-virus software looking for the original virus.
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 covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.
Workstation	A networked computer that uses server resources, a computer that is connected to a mainframe computer. It is usually a personal computer connected to a Local Area Network (LAN), which shares the resources of one or more large computers. They can have their own applications installed, as well as their own hard disks.
Worm	A worm is a more effective form of virus that finds vulnerable systems and then copies itself into those systems. The most frequent methods of propagation are from email distribution lists, email signature scripts, and shared folders on the network. Worms may or may not have a damaging payload. Currently the typical payload for a worm is making the computer more susceptible to other malicious viruses.