



TRINITY COUNTY PERSONNEL POLICY

SUBJECT:	Health Insurance Portability Accountability Act Policy (HIPAA)
POLICY NO.	15-05
INITIAL DATE PREPARED:	February 18, 2003
LAST DATE REVISED:	November 17, 2015
RESOLUTION NO.	N/A

TABLE OF CONTENTS

I.	PURPOSE	3
II.	APPLICATION	3
III.	DEFINITIONS	3
IV.	POLICY	6
V.	SEVERABILITY	9

I. PURPOSE

Trinity County is a hybrid entity and a covered entity and therefore subject to the Health Insurance Portability and Accountability Act ("HIPAA") of 1996. It is the purpose of this policy to ensure that Trinity County meets the compliance criteria to provide reasonable and appropriate administrative, technical, and physical safeguards to protect the privacy of Individually Identifiable Health Information ("IIHI") and;

- To better serve our customers, clients and consumers;
- To protect our employees from prosecution for failing to meet enforceable federal legislation;
- To fulfill our duty to protect the confidentiality and integrity of confidential medical information as required by law and professional ethics; and
- To support the general concept of the public's right to have more control over their personal information.

Compliance for HIPAA is promulgated through the national rule making process. Trinity County will continue in the review process as new rules are published or existing rules are amended.

II. APPLICATION

The county has within its service structure many departments and offices that receive, collect, store, use and transmit IIHI protected under Federal and State Laws. Individual departments have the responsibility to develop departmental policies, procedures and practices necessary to expand and tailor this overall County policy to the particular needs of their department. A department will not be considered HIPAA compliant until department-specific policies, procedures and practices are adopted as necessary in accordance with this County Policy.

Under HIPAA, those provisions of HIPAA concerning the privacy and confidentiality of a person's health confidential information "give way" to those California state law provisions, and other federal law provisions, that are more stringent than HIPAA.

County staff should follow California law or other federal law if it provides greater protection than HIPAA. If you are unsure which law to follow please contact County Counsel.

III. DEFINITIONS

A. Authorization

Authorization means the execution of a written document by the client, in order for the County to use or disclose IIHI in the fashion not clearly defined as "permitted use" under HIPAA.

Authorization must be obtained in advance except for emergency treatment. The authorization must be specific as to the information covered, who may disclose and receive that information,

and the use of the information, and include a "sunset" date specifying the end of the authorization period.

B. Business Associates

A Business Associate ("BA") is someone, either a person or other legal entity, who performs a function for a Covered Entity ("CE") involving the use, disclosure or creation of IIHI. The function performed does not have to be a covered function as defined in the Transaction and Code sets, but must be a function that the CE would have had to perform themselves.

C. Covered Entity

A health plan, a health care clearinghouse or a health care provider who transmits any health information in electronic form.

D. Enrollee

A health plan enrollee ("Enrollee") is any Covered Person enrolled in one or more of the group health plans sponsored by the County of Trinity, which results in the County of Trinity having possession of or access to protected health information.

1. When County of Trinity obtains protected health information about Enrollees, County of Trinity may use and disclose such protected health information consistent with federal and state law and regulation.

E. Hybrid Entity

Healthcare and associated activities are not the principal business of the County. Trinity County meets the definition of a "Hybrid Entity" under HIPAA. Some departments or units within departments will be designated as "covered functions" for purposes of HIPAA compliance. These designations are meant to reflect the activities that occur within a department and are not intended to restrict any activities. New activities that fall under the definition of covered functions, as they are identified, can be added to the list just as other activities that subsequently move outside the scope of HIPAA can be removed. A "Hybrid Entity" under HIPAA is also a "Covered Entity" for the purposes of compliance.

F. Limited Data Sets

For the purpose of sharing information, "Limited Data Sets" are defined as IIHI that excludes the following direct identifiers of the individual, or of relatives, employers or household members of the individual:

1. Names
2. Postal address information, other than town or city, state and zip code

3. Telephone numbers
4. Fax numbers
5. Electronic mail addresses
6. Social security numbers
7. Medical record numbers
8. Health plan beneficiary numbers
9. Account numbers
10. Certificate/license numbers
11. Vehicle identifiers and serial numbers, including license plate numbers
12. Device identifiers and serial numbers
13. Web Universal Resource Locators (URLs)
14. Internet Protocol (IP) address numbers
15. Biometric identifiers, including finger and voice prints, and
16. Full face photographic images and any comparable images

G. Minimum Necessary Confidentiality Information

1. County of Trinity will use or disclose only the minimum amount of confidential information necessary to provide services and benefits to HIPAA covered clients, and only to the extent provided in the County of Trinity privacy policy.
2. This policy does not apply to:
 - i. Disclosures to or requests by a health care provider for treatment;
 - ii. Uses or disclosures made to the individual;
 - iii. Uses or disclosures authorized by the individual;
 - iv. Disclosures made to the Secretary of the United States Department of Health and Human Services in accordance with federal HIPPA regulations at 45 CFR 160, Subpart C.
 - v. Uses or disclosures that are required by law; and
 - vi. Uses or disclosures that are required for compliance with federal HIPPA regulations at 45 CFR, Parts 160 and 164.
3. When using or disclosing an individual's confidential information, or when requesting an individual's confidential information from a provider or health plan, County of Trinity employees must make reasonable efforts to limit the amount of confidential information to the minimum necessary needed to accomplish the intended purpose of the use, disclosure, or request.

H. Notice of Privacy Practices

The Notice of Privacy Practices specifies client rights under HIPAA as well as the County Privacy Officer's contact information and the method of filing a complaint. This notice must be given to all clients, customers and patients of a department that provides a covered function and there must be a record that the individual was offered and/or received the notice. The notice

must be updated as necessary and the revised notice given to all existing or new clients, customers or patients.

I. Privacy

Privacy, for the purposes of this Policy, means the right to keep private and not disclose to other persons or entities.

J. Protected Health Information

For the purpose of these policies, the terms “confidential information”, “health confidential information”, individual health confidential information”, “protected health confidential information”, “protected health information”, “PHI”, “electronic protected health information”, and “ePHI” are the same. These terms mean information that:

1. Is a subset of health confidential information, including demographic confidential information collected from an individual, and
2. Is created, received, maintained, or transmitted by a health care provider, health plan, health care clearinghouse, or business associate; and
3. Relates to the:
 - i. Past, present, or future physical or mental health or condition of an individual; or,
 - ii. The provision of health care to an individual; or,
 - iii. The past, present, or future payment for the provision of health care to an individual; and
4. Either:
 - i. Identifies the individual; or,
 - ii. The confidential information creates a reasonable basis to believe it can be used to identify the person; and,
5. Is:
 - i. Transmitted by electronic media; or
 - ii. Maintained in electronic media; or
 - iii. Transmitted or maintained in any other form or medium, and
6. Does not include:

- i. Employment records; or,
- ii. Education records
- iii. Records under the Family Educational and Right to Privacy Act (FERPA).

K. Security

Security in this policy is defined as all measures taken by the County and its agents, contractors, officers and employees to insure that IIHI is protected in a manner compliant with the requirements of HIPAA and other State and Federal laws. Security includes but is not limited to, policies, procedures, practices, directives, manuals, training and methods as they relate to compliance with protection of IIHI. Security may also include mechanical and technological protections such as locks, secure access rooms and containers, computer hardware and software with security levels and protocols, secure communication devices and settings, and any other method, device or practice that limits improper access to IIHI.

III. POLICY

- A. Assessments: The County and its departments will continually assess their business practices in order to identify IIHI that should be protected. The assessment shall identify where IIHI is located, what is the purpose of the information, what legal mandates exist involving the collection/retention/use of the information, how the information is handled, how the information is shared or transmitted to other entities, and the final disposition of the information.
- B. Privacy Officer: The County will designate a Privacy Officer who is responsible for the development and implementation of the policies and procedures of the County relating to HIPAA rules. Information regarding the Privacy Officer is available at the Personnel Department.
- C. Steering Committee: Every department determined by the County HIPAA Steering Committee as engaging in activities covered by HIPAA, shall have a representative of their department assigned to the Steering Committee. The Department Head will designate a staff member within that department to serve on the Committee. The Committee will work with the County Privacy Officer to insure the department's compliance with HIPAA.
- D. Multi-Disciplinary Teams (MDTs): MDTs have the need to share client IIHI outside of their individual department, and occasionally outside the County system entirely. In order to share IIHI, an MDT will develop special authorization forms that clearly inform the client, when feasible, of the use and disclosure of information without hampering the functions of the law. The forms will be maintained and available with the effected departments.

- E. **Training:** Although not all departments within the County are "Covered" under HIPAA rules, in an attempt to reinforce the importance of confidentiality Countywide and to reduce risk, all employees will be trained on the County Privacy Policy at County initial orientation upon hire and at their annual reorientation thereafter. Employees will be required to sign a statement of understanding and/or a Confidentiality Agreement following the training.

Each department will be responsible for providing and documenting training provided to its employees on specific departmental policies, procedures and practices.

- F. **Security:** Pursuant to 164.530 of the HIPAA Privacy Rule, each department will develop policies, procedures and practices that will provide appropriate administrative, technical, and physical safeguards to protect the privacy of individually identifiable health information. The goals of the policies will be to reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards and to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

- G. **Departmental Policies and Procedures:** All Departments will develop and maintain written policies, procedures and practices that are necessary to be in compliance with the County Privacy Policy and the HIPAA Privacy Rule and will train their employees on these policies and retain records of training for audit purposes. The policies must be reasonably designed and take into account the size of and the type of activities that relate to IIHI used by the department. The County and departments must change policies and procedures as necessary and appropriate to comply with changes in the law pursuant to 164.530 of the HIPAA Privacy Rule.

While each department is responsible for monitoring its compliance with County policy, any infraction that appears to be systemic or repetitive will be reported to the County Privacy Officer for investigation. The County Privacy Officer will assist departments in developing plans and designing procedures that are HIPAA-compliant. The HIPAA Privacy Officer may, in his or her discretion, audit and examine the procedures and practices of any department to ascertain compliance with the requirements of this policy.

- H. **Sanctions and Penalties:** There are civil and/or criminal penalties imposed by the Federal Government for the misuse or disclosure of IIHI with fines that range from \$100 to \$250,000 and up to 10 years in prison. In addition, the County will impose progressive discipline in accordance with Article X, Disciplinary Procedures of the Trinity County Code for failure to comply with County or departmental HIPAA policies. The following four areas may be cause for applying sanctions to an employee:

1. Failure to comply
2. Wrongful use or disclosure of IIHI
3. Violations of relevant state or federal law
4. Violations of Trinity County or departmental policies and procedures as they relate to HIPAA

- I. **Allowable Uses and Disclosures:** In general, subject to specified limitations outlined in Section 164.502 through 164.514 of the HIPAA rule and more stringent State and Federal laws, each covered function within the County may use or disclose Protected Health Information for purposes of treatment, payment and general operations. Each covered function within the County will develop policies and procedures to comply with applicable State and Federal laws and HIPAA regulations in the area of uses and disclosures of IIHI. A procedure and practice for an accounting of disclosures will be developed and maintained pursuant to Section 164.528 for the HIPAA Privacy Rule with the personnel director.
- J. **Complaints and Whistleblowers:** Individuals or whistleblowers can report suspected violations of HIPAA policy to the County Privacy Officer. These complaints can be made anonymously and retaliatory actions cannot be taken against complainants. The County Privacy officer will attempt to mitigate, to the extent practicable, any harmful effect resulting from a violation of HIPAA rules. The complaints and resolutions will be documented and retained for six years.
- K. **Access:** Each covered function within the County will establish a policy and procedure for individuals for their personal representative to access, inspect, obtain a copy of and amend protected health information about the individual in a designated record set and with certain exceptions as described in Sections 164.524 through 164.526 of the HIPAA Privacy Rule and State or Federal law.
- L. **Business Associates:** All BA's of the County will safeguard any IIHI it creates or retains on the County's behalf. The County will be assured of the safety of the IIHI by means of contractual obligations for BA. County Counsel will monitor all contracts to identify BA who are subject to HIPAA regulations. If the County becomes aware of non-compliance with HIPAA regulations on the part of a BA, the County will terminate the contract or report the problems to the Secretary of the U.S. Department of Health and Human Services.
- M. **Notice of Privacy Practices:** County will develop a Notice of Privacy Practices for distribution to all individuals who receive services. The notice will include the uses and disclosures of protected health information that may be made by the covered entity and of the individual's rights and the covered entity's legal duties with respect to protected health information. The notice is subject to the exceptions and requirements described in Sections 164.520 through 164.528 of the HIPAA Privacy Rule.

IV. SEVERABILITY

In the event any provision of this Policy is declared by a court of competent jurisdiction to be illegal or unenforceable, that policy provision shall be null and void, but such nullification shall not affect any other provision of the Policy, which shall remain in full force and effect.

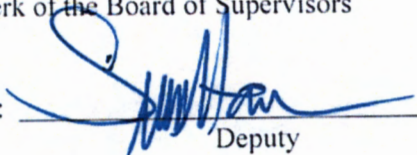
DULY PASSED AND ADOPTED this 17th day of November, 2015 by the Board of Supervisors of the County of Trinity.



JUDY MORRIS, CHAIRMAN
Board of Supervisors
County of Trinity
State of California

ATTEST:

WENDY G. TYLER
Clerk of the Board of Supervisors

By: _____
Deputy

**ACKNOWLEDGMENT OF REVIEW
BY TRINITY COUNTY EMPLOYEES**

I have received and read a copy of the Trinity County Privacy Policy and Procedures consisting of nine pages and this acknowledgment page. I understand that all individuals, including volunteers and interns, performing work and/or services for the County or observing health care practices as part of an internship or other program are required to observe standardized privacy and security practices, as outlined in the County Privacy Policy and Procedures and HIPAA Training Modules, with respect to the use and disclosure of individuals' protected health information created, acquired and maintained by the County. I agree to abide by these policies and procedures.

Employee Signature

Date