County of Yolo
Administrative Policies and Procedures Manual

TITLE: PRIVACY & SECURITY	DEPARTMENT: COUNTY ADMINISTRATIVE OFFICE
TYPE: **POLICY**	DATE: SEPTEMBER 13, 2011

A. Purpose

1. In order for Yolo County to meet the compliance criteria of the 1996 Health Insurance Portability Accountability Act (HIPAA), to better serve our clients, to protect our employees from prosecution for failing` to meet enforceable federal legislation, and to support the general concept of the public's right to have more control over their personal information, we adopt the following policy.

2. Compliance for HIPAA is promulgated through the national rule-making process. The HIPAA Privacy Rule and Security Rule and the Health Information Technology for Economic and Clinical Health Act (HITECH) apply to this Policy.

3. This policy is written for the purpose of defining what health or health related information is considered private and what constitutes privacy and security within the County, outlining our clients rights regarding privacy, giving a detailed process for reporting violations, identifying the HIPAA Privacy and Security Officer, and providing guidelines for employee training in privacy and security.

4. This Policy applies to the County workforce, including officers, employees, agents, contractors, etc. when acting in the course and scope of their work for the County, and also when acting in a private capacity if that involves any information obtained while working on County-related matters. (For example, if confidential information is obtained in the course and scope of working for the County, it remains confidential, and must be kept confidential, when the individual is otherwise acting in a private capacity (e.g., traveling with County information in computers, CDs, notebooks, etc.; discussions with family members, friends, etc.; internet communications, "blogging," etc.)

5. Nothing in this Policy shall be construed as relieving departments of the responsibility to develop full and complete departmental policies, procedures and practices necessary to expand and tailor this overall County policy to the peculiar needs of their department. A department will not be considered HIPAA-compliant until department-specific policies, procedures and practices are adopted supplemental to this Policy.

B. County Privacy and Security Officer

1. The County Privacy and Security Officer shall oversee and assist Yolo County's efforts to comply with HIPAA and this Policy, including but not limited to assisting Yolo County departments in complying with HIPAA and this Policy; designating the covered health care components of the County's hybrid entity; developing sample notices and forms as required by HIPAA or this Policy; receiving complaints of alleged HIPAA violations at the County-wide level and assisting in the investigation and resolution of such complaints; serving as the County's primary point of contact for the United States Secretary of Health and Human Services regarding HIPAA;

providing, securing or assisting in the training of members of the County workforce regarding HIPAA and this Policy; assisting department privacy and security liaisons in developing and implementing departmental administrative, physical, and technical safeguards; keeping current with changes in HIPAA legislation and requirements; and performing other functions and tasks as described in this Policy or as otherwise designated by the County Administrative Officer. In fulfilling the duties, responsibilities, obligations, rights and responsibilities as County Privacy and Security Officer, he/she shall be subject to the review, direction and control of the County Administrative Officer (or designee).

2. The County Privacy and Security Officer shall submit and present written activity and compliance reports quarterly to the County Administrative Officer and annually to the Board of Supervisors, and more frequently if necessary under the circumstances.

C. Department Privacy and Security Liaison

1. Every department determined by the County Privacy and Security Officer as engaging in activities covered by HIPAA, shall have a department privacy and security liaison. The head of the department may appoint him or herself, or a staff member within that department, to serve as the department's privacy and security liaison. The department privacy and security liaison shall work with the County Privacy and Security Officer to ensure the department's compliance with HIPAA, including but not limited to assisting his or her department in complying with HIPAA and this Policy; evaluating department activities within the covered health care components of the County's hybrid entity; developing sample notices and forms as required by HIPAA or this Policy for the department's use subject the review and approval of the County Privacy and Security Officer; receiving complaints of alleged HIPAA violations at the department-wide level and assisting in the investigation and resolution of such complaints; serving as the department's primary point of contact for the County Privacy and Security Officer regarding HIPAA; providing, securing or assisting in the training of members of the department's workforce regarding HIPAA and this Policy; developing and implementing departmental administrative, physical, and technical safeguards; keeping current with changes in HIPAA legislation and requirements; and performing other functions and tasks as described in this Policy or as otherwise designated by the County Privacy and Security Officer.

D. Definitions

1. Hybrid Entity.

   a. A "Hybrid Entity" under HIPAA is also a "Covered Entity" for the purposes of compliance. Yolo County meets the definition of a "Hybrid Entity" under HIPAA because, while the County participates in some activities that meet the definitions of healthcare plan and healthcare provider that are covered by HIPAA, none of those activities is the principal

business of the County. In addition, some administrative and support services provided to County healthcare plan or healthcare provider activities by County departments (e.g., auditing and accounting, legal, quality assurance and oversight, etc.) would qualify as "business associate" activities if performed by a separate legal entity.

b. Based upon these activities, some departments or units within departments will be designated as "covered components" 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 components, 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.

c. Subject to the direction and control of the County Administrative Officer or her/his designee ("CAO"), the County Privacy and Security Officer shall designate the operations of all or part of any County department as a covered component or a non-covered component, and revise such designations from time-to-time as may be necessary or appropriate pursuant to HIPAA. The County Privacy and Security Officer shall maintain adequate documentation and explanation of all such designations and the basis of such designations.

d. Each covered department or component shall implement physical, administrative and technical safeguards, approved by the County Privacy and Security Officer**,** to prevent the use or disclosure of protected health information within departments, between departments, and within departments that have covered components and non-covered component, except to the extent that such use or disclosure is authorized by law. Safeguards shall reasonably ensure the privacy and security of protected health information, and prevent that information from being obtained, used or disclosed by non-authorized personnel, components and departments.

2. Privacy

a. Privacy includes maintaining the confidentiality of health information that would specifically identify an individual or through the information a reasonable person could deduce whom the information is about, when that information is included with other information that would indicate the past, present or future physical or mental health or condition of the individual; the provision of health care to the individual; or the past, present, or future payment for the provision of health care to the individual. The two pieces of interlocked information are considered Protected Health Information (PHI), which is covered by the HIPAA Privacy Rule; if the PHI is created, collected, used, maintained or transmitted in electronic form Electronic Protected Health Information, "EPHI", it is covered by the HIPAA Security Rule. The HIPAA Privacy Rule and Security Rules are the focus of this Policy.

b. Some information may look like PHI, but in fact not be a part of the enforceable section of HIPAA. Given competing interpretations, conflicts in legislation and regulation, and general

difficulty in assessing what PHI is in the absence of precedent, Yolo County pursues a conservative approach in the designation of PHI, and will define information as PHI unless it can be clearly demonstrated that said information is outside the scope of PHI as defined by HIPAA.

3. Security.

   a. Security is defined as all measures taken by the County and its agents, contractors, officers and employees to ensure that PHI, EPHI, and other sensitive information is reasonably protected, accurate and accessible in a manner that complies with the requirements of HIPAA. This requires the adoption and implementation of administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of PHI, EPHI, and other sensitive information from unauthorized access, alteration, deletion, or transmission

   b. Security includes, but is not limited to, reasonable policies, procedures, practices, directives, manuals, training, and methods that limit improper access to PHI. 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 PHI or renders it unusable, unreadable, or indecipherable to unauthorized individuals throughout the use of a technology or methodology.

   c. Cautious consideration must be given to allowing offsite use and access to EPHI. With the advent of technology that allows for easier access to the County's network, the level of risk for loss of devices and hacking from unauthorized users has grown. Need for access must be evaluated to determine risk and management strategies, procedures for safeguarding EPHI, and the level of security awareness and training needed prior to remote access. Remote access to EPHI should only be granted to authorized users based on their role within the organization and their need for access to EPHI and only if they comply with policy and procedures described here and within the County Network Policy.

   d. This includes (but is not limited to):

      (1.) Administrative Safeguards, such as: Security Management (e.g., Risk Analysis and Management, Network Security Policy), Workforce Security (e.g., Workforce Access Clearance and Termination Procedures), Security Incident Procedures (Response, Reporting, and Remediation), and Contingency Planning (e.g., Data Backup, Disaster Recovery, and Emergency Operations);

      (2.) Physical Safeguards, such as Workstation Use and Security, and Electronic Device and Media Use, Re-Use and Disposal; and

(3.) Technical Safeguards, such as Access Control (e.g., Unique User Identification and Authentication), Emergency Access Procedures, and Periodic Audits and Compliance Reviews.

e. The County Information Technology policies will incorporate necessary HIPAA and Health Information Technology for Economic and Clinical Health **(**HITECH**)** Act safeguards and security protections in conformance with this Policy for those systems that are managed by the Department of Information Technology & Telecommunications. Departments managing their own systems must develop their own necessary and appropriate safeguards and security protections that comply with HIPAA and prevent, detect, contain, and correct security violations.

4. Business Associate Designation.

a. A Business Associate (BA) (under HIPAA) or Qualified Service Organization (QSO) (under 42 Code of Federal Regulations, Part 2) is a person or legal entity that performs a function for a Covered Entity (CE) involving the use, disclosure or creation of PHI. Examples of services that a BA/QSO can provide include: data processing, case management, dosage preparation, laboratory analyses, vocational counseling, patient transportation, medical and health care, and legal, accounting or other professional services. The function performed does not have to be a covered function as defined in HIPAA. As directed by the HITECH Act, Business Associates are required to comply with many aspects of the HIPAA Privacy and Security Rules. This requirement means BAs must develop reasonable physical, technical, and administrative safeguards to protect PHI and must implement written policies and procedures with respect to such safeguards. The County Privacy and Security Officer will develop sample BA/QSO contract language in consultation with County Counsel.

5. Authorization.

a. Authorization means the execution of a written and legally sufficient document by the client authorizing the County to use or disclose PHI in a fashion not otherwise clearly defined as a "permitted use" or "permitted disclosure" under HIPAA.

E. <u>Allowable Uses/Disclosures of PHI (Without Authorization)</u>

1. In general, and subject to the specific limitations outlined below, without an authorization Yolo County, its officers, agents, employees and contractors may <u>not</u> use or disclose PHI except in the circumstances set forth below. However, the application of each of these exceptions is subject to significant qualifications and limitations; consequently, before releasing or using PHI pursuant to any of these exceptions staff must consult with the department privacy and security liaison.

a. For Uses/Disclosures that are specified in the Notice of Privacy Practices:

(1.) To the individual (no minimum necessary required);
[45 C.F.R. 164.502(a)(1)(i)]

(2.) Treatment (no minimum necessary required);
[45 C.F.R. 164.502(a)(1)(ii)]

(3.) Payment to another covered entity;
[45 C.F.R. 164.502(a)(1)(ii)]

(4.) Health care operations within the County's Hybrid Covered Entity;
[45 C.F.R. 164.502(a)(1)(ii)]

(5.) To participants of a organized health care arrangement;
[45 C.F.R. 164.502(a)(1)(v)]

(6.) Pursuant to a valid authorization; and
[45 C.F.R. 164.502(a)(1)(iv)]

(7.) When required by the United States Secretary of Health and Human Services to investigate compliance (no minimum necessary required).
[45 C.F.R. 164.502 (a)(2)(ii];

(8.) In the case that a covered entity uses or maintains an electronic health record with respect to protected health information—

a. ''(A) the exception under paragraph 164.528 of title 45, Code of Federal Regulations (a)(1)(i) of such section shall not apply to disclosures through an electronic health record made by such entity of such information; and

b. ''(B) an individual shall have a right to receive an accounting of disclosures described in such paragraph of such information made by such covered entity during only the three years prior to the date on which the accounting is requested.
[§ 13405(c)(4)(A];

b. For uses or disclosures required by law (no minimum necessary required);
   a. [45 C.F.R. 164.502(a)(2)(v)}

c. To a business associate (if safeguarded by a business associate agreement);
   a. [45 C.F.R. 164.502 (e)]

d. To another government agency when administering a public benefit health plan;

a. [45 C.F.R. 164.502(e)(1)(ii)(C)]

e. By whistleblowers if to an oversight agency or attorney based on belief of HIPAA violation;
   a. [45 C.F.R. 164.502(j)]

f. If and only if the individual has been given an opportunity to protest in advance, PHI may be disclosed for the following purposes:

(1.) Facility directories;
[45 C.F.R. 164.510(a)]
(2.) Family members, other relatives or a close personal friend;
[45 C.F.R. 164.510(b)]
(3.) Directly related PHI in emergency situations;
[45 C.F.R. 164.510(b)(3)]
(4.) Disaster relief purposes;
[45 C.F.R. 164.510(b)(4)];

g. To the extent required by law;
[45 C.F.R. 164.512(a)]

h. For public health activities authorize by law;
[45 C.F.R. 164.512(b)]

i. To report abuse or neglect as authorized by law;
[45 C.F.R. 164.512 (c)]

j. To the FDA with respect to regulated product or activities;
[45 C.F.R. 164.512 (b)(3)]

k. To a person who may have been exposed to a communicable disease;
[45 C.F.R. 164.512 (b)(4)]

l. To an employer if the employer is a covered health care provider of the employee;
[45 C.F.R. 164.512 (b)(v)]

m. Public health activities if the covered entity is a public health authority;
[45 C.F.R. 164.512(a)(ii)]

n. To a government authority PHI about an individual believe to be a victim of abuse, neglect or domestic violence;
[45 C.F.R. 164.512 (c)]

o. To a health oversight agency for activities authorized by law;
[45 C.F.R. 164.512(d)]

p. 16) In the course of any judicial or administrative proceeding, if receive satisfactory assurance, from the party seeking the information, that reasonable efforts have been made by such party to ensure that the individual who is the subject of the requested PHI has been given notice of the request, or the party seeking the information has made reasonable efforts to secure a qualified protective order;
[45 C.F.R. 164.512(e)]

q. For law enforcement purposes;
[45 C.F.R. 164.512(f)]

r. To a coroner or medical examiner for duties authorized by law;
[45 C.F.R. 164.512(g)]

s. To organ procurement organizations;
[45 C.F.R. 164.512(h)]

t. For research if authorized by an IRB or privacy board;
[45 C.F.R. 164.512(i)]

u. If necessary to avert a serious threat to health or safety;
[45 C.F.R. 164.512(j)]

v. For specialized government functions;
[45 C.F.R. 164.512(k)]

w. For military and veterans activities;
[45 C.F.R. 164.512(k)(1)]

x. For correctional institutions or other law enforcement custodial situations;
[45 C.F.R. 1647.512 (k)(5)]

y. For government programs providing public benefits;
[45 C.F.R. 164.512(k)(6)]

z. For worker's compensation;
[45 C.F.R. 164.512(k)(7)]

aa. As a limited data set that meets the requirements of law;
[45 C.F.R. 164.514(e)]

bb. For fundraising; and
[45 C.F.R. 164.514(f)]

cc. For underwriting and related purposes.
[45 C.F.R. 164.514(g)]

2. No County personnel, business or contractor will use or disclose protected health information for marketing purposes unless specifically authorized by the County Administrative Officer and the covered entity has obtained the patient's authorization prior to sending the marketing communication.

F. <u>Authorization</u>

1. An authorization must be obtained before using or disclosing PHI in a fashion not otherwise clearly defined as a permitted use or disclosure under HIPAA. Authorization must be obtained in advance except for emergency treatment.

2. The authorization must be specific as to the information that may be disclosed, who may disclose and receive that information, the permitted use of that information, and include an expiration date for the authorization. A separate authorization is required to release psychotherapy notes.

3. The County Counsel and County Privacy and Security Officer have developed a sample form for a client to grant authorization. Each individual department will need to develop an authorization form (or forms) appropriate for that department's circumstances and operations in a manner that complies with HIPAA, while also making such modifications as may be necessary to take into account the specific laws and regulations that apply to that department's personnel, operations and circumstances. Each department shall file a copy of its authorization(s) with the County's Privacy and Security Officer, including all revisions.

4. Multiple Disciplinary Teams (MDTs) have the need to share client PHI outside of their individual department, and occasionally outside of the County system entirely. Unless otherwise authorized by HIPAA (as identified by the MDT, and confirmed by the County Privacy and Security Officer), in order to share PHI between MDT members and participants an MDT will have to develop special authorization forms that clearly informs the client of the use and disclosure of information, and complies with HIPAA as well as the specific laws and regulations that apply to that MDT's personnel, operations and circumstances.

5. It should be noted that some programs in the health and human services departments use other types or forms of "authorizations" for program purposes in circumstances in which it is not required by HIPAA, but is required by other applicable laws, regulations or standards or practice. All authorizations must nevertheless meet the County standard.

G. Access to PHI

1. Each department shall establish reasonable methods of verifying the authority and identity of an individual seeking access to protected health information, and shall establish procedures for documenting that such verification was obtained before each instance of releasing such information. All access requests shall be documented regardless of whether PHI was released or not.
2. Each department must implement and maintain necessary and appropriate means to secure and protect health data, including data transmitted via email, direct connection to county networks, and FAX. Measures may include, but are not limited to encryption, use of closed County networks, and appropriate measures of ensuring privacy while using a computer, smart phone, or FAX machine.
3. No department policy or procedure may subvert minimum and necessary aspects of this County policy or procedure.

H. Minimum Necessary

1. Generally speaking, when using or disclosing protected health information or when requesting protected health information from another covered entity, reasonable efforts must be made to limit the use or disclosure of the protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. This requirement does not apply to disclosures to or requests by a health care provider for treatment; uses or disclosures made to the individual or pursuant to an authorization (unless the was initiated at the County's request); disclosures made to the DHHS Secretary in accordance with HIPAA; and some (but not all) uses or disclosures that are required by law.
2. Rules prohibit the sale of Electronic Health Records (EHR) or PHI by a Covered Entity without the individual's expressed consent, however remuneration can be collected for the limited purposes of: (i) public health activities, (ii) research (for cost of preparing and transmitting), (iii) treatment, (iv) sale, transfer, merger, or consolidation with another Covered Entity, (v) providing a business Associate with remuneration under a Business Associate Agreement, and (vi) providing an individual access to his or her PHI as long as the costs do not exceed actual costs of preparing and transmitting the information.

I. Internal Review, Assessment and Planning

1. In order to identify what needs to be included for privacy protection, a department-by-department review and assessment is necessary. The review assessment shall identify and locate all PHI maintained by the department, determine the lawful and appropriate purposes of having the information; determine all legal mandates regarding the collection, use, retention and disposition of the information; determine how the information is currently collected, handled, used, retained and disposed of; and determine how the information is shared with and transmitted to other entities, if at all. Use of records for staff training, privacy breaches, incidents, and authorized

staff access to PHI will be reviewed. The review and assessment examines and evaluates a department's or departmental unit's entire business process as it relates to or affects PHI.

2. After the initial review and assessment is performed, a second assessment is made to identify any information that will be transmitted electronically ("EPHI"), and then to gather the same information noted above for that EPHI. (The electronic transmission of PHI may also mean that the information is subject to the Transaction and Code Sets Rule.) Any system for collecting, handling, using, transmitting retaining and disposing of the EPHI must comply with HIPAA.

3. The information obtained from each review and assessment must then be documented in writing.

4. Upon completion of all reviews assessments, and documentations, the department privacy and security liaison must then, in conjunction with the County Privacy and Security Officer, combine all information into a Review and Assessment Report and Implementation Plan for the department or unit. The implementation should address how the department or unit will comply with HIPAA as well as other applicable laws and regulations, including any remediation necessary for such compliance. While remediation is intended to eliminate or mitigate County risk, it is not the intention of this Policy to make compliance so difficult as to hinder the County's myriad responsibilities under other laws and regulations. The Review and Assessment Report and Implementation Plan become part of the documentation for compliance with HIPAA and other applicable laws and regulations (including but not limited to audit compliance). The department privacy and security liaison shall periodically repeat the review and assessment, and then update the Report and Plan as necessary and appropriate to comply with HIPAA and other applicable laws and regulations. The department privacy and security liaison shall also forward a copy of the Report and Plan to the County Privacy and Security Officer (including any revisions).

J. <u>Notice of Privacy Practices</u>

1. The County shall develop, update from time-to-time as appropriate, and distribute a "Yolo County Notice of Privacy Practices" that generally specify the uses and disclosures of protected health information that may be made by the County's covered components, the individual's rights and the County's legal duties with respect to protected health information, and the County Privacy and Security Officer's contact information and the method of filing a complaint. Each individual department shall develop, update from time-to-time as appropriate, and distribute a notice (or notices) of privacy practices appropriate for that department's personnel, operations and circumstances in a manner that complies with HIPAA, making such modifications to the County's Notice as may be necessary to take into account the specific laws and regulations that apply to that department's personnel, operations and circumstances. Each department shall file a copy of its notice(s) of privacy practices with the County's Privacy and Security Officer, including all revisions.

2. Each department program that constitutes a "health care provider" or "health plan" in accordance with HIPAA must give its notice of privacy practice to its clients at the time that services are first provided to the client, or as soon thereafter as is practical under the circumstances. In addition, health plans must also give the notice not less frequently than once each three (3) years.

K. Client Rights

1. County clients have the following rights:

   a. The right to request restrictions on certain uses and disclosures of protected health information, as provided by Sec. 164.522(a); however, the covered component is not required to agree to a requested restriction; (i) unless it relates to disclosures to a health plan for payment and/or health care operation and (ii) the PHI relates to a health care service or product that for which the individual has paid out of pocket and in full.

   b. The right to receive confidential communications of protected health information in any reasonable time, place and manner, as provided by Sec. 164.522(b);

   c. The right to inspect and copy protected health information in a designated record set, as provided by Sec. 164.524;

   d. The right to seek an amend of protected health information in a designated record set, as provided by Sec. 164.526;

   e. The right to receive an accounting of certain disclosures of protected health information, as provided by Sec. 164.528;

   f. The right to obtain a paper copy of the notice of privacy practices from the covered entity upon request including an individual who has previously requested or agreed to receive the notice electronically, as provided by Sec. 164.520;

   g. The right to file a complaint, as provided by Secs. 160.306 and 164.530; and

   h. The right to be free from retaliation for filing a complaint, as provided by Sec. 164.530.

L. Breach Notification

1. In the event of a breach of PHI which "poses a significant risk of financial, reputational, or other harm to the individual," the department must report the breach as soon as possible to the Privacy and Security Officer, completing an Incident Report Form describing the breach no later than 3 business days following the breach. A sample Incident Report Form is attached to this Policy.

2. In the event of a breach, the Covered Entity must undertake a risk assessment and determine in good faith if it is necessary to notify individuals of the breach. In addition to notifying individuals, the breach must also be reported to the Secretary of the Department of Health and Human Services, and in some instances, the media.

3. In the event of a release of unsecured PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals, the Covered Entity or Business Associates must notify individuals whose unsecured PHI has been or is reasonably believed to have been, acquired, accessed, used, or disclosed in a manner that compromises the security, privacy, or integrity of the PHI.

M. Complaints

1. Any person or entity who believes that the County, any member of the County's workforce, or any County Business Associate, has violated or is otherwise not complying with the Privacy and Security requirements of HIPAA or this Policy may submit a complaint. A compliant may be submitted verbally or in writing, but it is encouraged that a verbal complaint be followed-up by a written complaint. A Sample Complaint Form (written) is attached to this Policy.

2. Any person may submit an anonymous complaint; however, that may limit the ability to thoroughly investigate the complaint. If a complaint is submitted with a request that it be kept confidential, the information provided will remain confidential to the extent feasible; however, in some circumstances information will need to be disclosed in order to properly investigate the complaint.

3. Any such complaint may be submitted to any County supervisor, manager, or administrator, including but not limited to the County Administrative Officer and County department heads. A complaint may also be submitted to any County department privacy and security liaison, or to the County's Privacy and Security Officer

4. Individuals, the public and whistleblowers may also file their complaint with the Secretary of the U.S. Department of Health and Human Services (DHHS) at:
   Office of Civil Rights
   U.S. Department of Health and Human Services
   200 Independence Avenue, SW, HHH Bldg., Room 509H
   Washington, D.C. 20201
   Phone: (886) 637-7748 TTY: (996) 78804989
   Email: www.hhs.gov/ocr

5. The specific duties of the County Privacy and Security Officer regarding complaint include, but are not limited to:

a. Receiving complaints from individuals concerning violations of HIPAA or this Privacy and Security Policy, or both;

b. Logging all complaints received and tracks the disposition of the complaints;

c. Reviewing complaints for allowable uses and disclosures, and summarily disposing of complaints that identify allowable uses and disclosures;

d. Reviewing complaints for non-HIPAA related issues and referring the individuals to the appropriate organization, if any;

e. Identifying the type of all HIPAA-related complaints including allegations of: Inappropriate use or disclosure of Personal Health Information (PHI); Inappropriate disposal of PHI; Denial of access to PHI; Denial of amendments to PHI;

f. Identifying where and against whom complaints have been lodged;

g. Investigating the complaints;

h. Conducting a risk assessment to determine the significance of the risk to the individual's finances, reputation, or suffering other harm. The risk assessment will include interviews, examination of facilities, materials, and documentation.

i. Coordinating and collaborating with department privacy and security liaison and other members of the workforce to investigate complaints and develop proposed resolutions (including but not limited to changes in business practices or information technology changes; personnel actions; contract changes or terminations, etc., where appropriate);

j. Informing the individual of the proposed resolution of the complaint;

k. Serving as the County's liaison with the federal and/or state government with respect to any inquiries regarding HIPAA, including but not limited to privacy and security complaints; and

l. Reporting all actions, decisions, and procedures related to complaints to the County Administrative Office.

N. <u>No Retaliation</u>

1. No person shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual or organization that exercises any rights granted by HIPAA or recognized in this Policy, including but not limited to filing a complaint or assisting in the lawful investigation of such a complaint, or opposing any act or practice made unlawful by HIPAA or

otherwise prohibited by this Policy, provided the individual or person has a good faith belief that the practice opposed is unlawful or violates this Policy, and the manner of the opposition is reasonable and does not involve a disclosure of protected health information in violation of HIPAA or this Policy.

O. Corrections, Sanctions and Penalties

2. The Corrections and Sanction Process, which is required by HIPAA, is the first defense in protecting the Yolo County workforce from penalties for violating HIPAA. This Process is intended to protect employees and contractors by providing progressive responses proportionate to the nature of the infraction. Enforcement of sanctions may not be used to harass employees, but may be a component of the employee performance review process (as are other violations of County policies and procedures and applicable laws and regulations). The HIPAA Privacy Rule and subsequently the HITECH Act Subtitle D provide the following sanctions and penalties. Note: HIPAA criminal penalties remain in effect and are not affected by changes to the civil penalties described in the HITECH Act; Criminal charges will be prosecuted by State Attorneys General.

a. Penalties for Wrongful Disclosures per the Privacy Rule:

(1.) Committed knowingly: imprisonment of not more than one (1) year, or both;

(2.) Committed under false pretenses: imprisonment of not more than five (5) years, or both; and

(3.) Committed with intent to sell, transfer, or use IIHI for commercial advantage, personal gain, or malicious harm: imprisonment of not more than ten (10) years, or both.

3. Civil Penalties range from $100 to $50,000 per HIPAA violation and are levied by the Secretary of Health and Human Services

a. A violation without knowledge of the violation - $100 per violation, with an annual maximum amount of $25,000 in penalties.

b. A violation that is due to reasonable cause - $1,000 per violation, with an annual maximum amount of $100,000 in penalties.

c. A violation that is due to willful neglect-$10,000 per violation, with an annual maximum amount of $1,500,000 in penalties.

4. In addition, the County may impose sanctions for violations of policy, practices or other applicable laws and regulations, including but not limited to the following:

   a. Failure to Comply;

   b. Wrongful Use or Disclosure of PHI;

   c. Violation of relevant state law; or

   d. Violation of Yolo County's policies and procedures as they relate to privacy and security, including but not limited to HIPAA.

   e. In the event of a sanctioning event as specified above, the County may impose any or all of the following corrective and/or disciplinary actions:

      (1.) Informal corrective action, including encouragement and recognition, verbal instruction, and additional training;

      (2.) Informal counseling and, when appropriate, referral to the Employee Assistance Program;

      (3.) Corrective interview, documented;

      (4.) Formal letter of reprimand;

      (5.) Reduction in pay;

      (6.) Suspension with or without pay;

      (7.) Demotion; or

      (8.) Dismissal.

P. <u>Audit and Compliance</u>

1. While each department is responsible for monitoring its compliance with this Policy, each department shall also report any infraction of this Policy that appears to be systemic or repetitive to the County Privacy and Security Officer for investigation. The County Privacy and Security Officer will assist departments in developing compliance plans and in designing procedures that are HIPAA-compliant.

HEALTH AND MEDICAL INFORMATION
HIPAA PRIVACY AND SECURITY
COMPLAINT FILING FORM

	DATE:	FILE NUMBER:

The information you provide here will remain confidential to the extent possible, however we may need to divulge some the information to investigate your claim. Anyone may file a complaint. Members of the workforce may use this form to report violations of HIPAA by others in the workforce.

You may submit your complaint to: any County supervisor, manager or administrator, including but not the County Administrative Officer and County department heads. You may also submit your complaint to any County department privacy and security liaison, or with the County's Privacy and Security Officer, David Nelson Yolo County Privacy & Security Officer, 10 Cottonwood, Woodland, CA 95695, Telephone: (530) 666-8958; FAX: (530) 666- 8975.

1. YOUR INFORMATION

LAST NAME:	FIRST NAME:	MIDDLE INITIAL:
ADDRESS:	CITY/STATE:	ZIP CODE:
EMAIL ADDRESS:	DAYTIME TELEPHONE NUMBER:	EVENING TELEPHONE NUMBER:
BEST WAY TO REACH YOU:	BEST HOURS TO REACH YOU:	

EMPLOYEES ONLY	**EMPLOYEES MAY FILE COMPLAINTS ANONYMOUSLY**	UNIT TITLE:	SUPERVISOR'S NAME:

2. INFORMATION ABOUT YOUR COMPLAINT

NAME OF THE ORGANIZATION YOUR COMPLAINT IS AGAINST:	NAME OF PERSON YOUR COMPLAINT IS AGAINST:	DATE YOU FIRST NOTICED ACTION THAT YOU ARE COMPLAINING ABOUT:	DATE(S) ACTION(S) OCCURRED:

HEALTH AND MEDICAL INFORMATION PRIVACY COMPLAINT FILING

(Continued)

DETAILS OF THE COMPLAINT:

I have reason to believe that one or more of the following has occurred:

- ☐ The organization/person has inappropriately disclosed my personal health information
- ☐ The organization/person has inappropriately used my personal health information
- ☐ The organization/person has inappropriately disposed of my personal health information
- ☐ The organization/person has denied access to my personal health information
- ☐ The organization/person has denied my amendment to my personal health information
- ☐ The organization's privacy policies and procedures violate HIPAA requirements
- ☐ Other: _____

Please provide a detailed description of your complaint covering *what, when, who, how, where, and if you know, why* about what happened. Please list any harmful affects you know of from what happened. You may attach additional pages if there is not enough space here.

DO YOU HAVE WITNESS(ES): ☐ NO ☐ YES

If yes, please provide the names, addresses and telephone numbers of your witness(s) below (Please attach additional pages if there is not enough space here):

WITNESS NAME:	ADDRESS:	TELEPHONE NUMBER:
WITNESS NAME:	ADDRESS:	TELEPHONE NUMBER:

3. REQUESTED RESOLUTION OF YOUR COMPLAINT

PLEASE DESCRIBE HOW YOUR PRIVACY COMPLAINT COULD BE RESOLVED:

4. YOUR SIGNATURE

SIGNATURE:	DATE:

Protected Health Information (PHI) Breach Incident Report Form

Complete this form when security breaches or incidents are suspected. Security breaches or incidents may include detection of viruses, worms, or other malicious code; loss of storage media; or other disclosures of PHI. Contact the Privacy and Security Officer if it is determined that a violation has occurred. File this report.

Breach Description

1. Date of the breach or incident -
2. Breach or incident location -
3. Persons involved in the breach or incident -
4. Description of breach or incident by the person(s) involved – include how the breach or incident occurred, the data media type, computer system type, malfunctioning symptoms, results, and any other information regarding the breach or incident. (*Attach additional pages as needed.)*

Breach Investigation **Investigation Performed by:**

1. Was PHI released or compromised that could be used to reasonably identify an individual(s)?

2. Does information released or compromised relate to the past, present, or future medical condition of the individual(s)?

3. Does the information involved in the breach or incident relate to the payment of healthcare for the individual?

4. Did the breach or incident pose "a significant risk of financial, reputational, or other harm to the individual(s)" impacted?

5. Specify the type(s) of information involved in the breach or incident. **(Check all that apply)**

	First Name		**Last Name**		**Claims Info**		**Other Financial info**
	Address/Zip		**Date of Birth**		**Diagnosis/Condition**		**Medications**
	SSN		**Driver's License**		**Lab Results**		**Other Treatment Info**
	Other Identifier		**Credit Card No.**		**Other**		

Add any other type of information-

6. Specify any safeguards in place prior to or during the incident. (Check all that apply)

	Firewalls		**Packet Filtering**		**Secure Browser**		**Strong Authentication**
	Encryption		**Physical Security**		**Logical Access Control**		**Anti-virus Software**
	Intrusion Detection		**Biometric Access Equipment**		**HIPAA Training**		**Other**

Add any other safeguards –

Data Recovery

7. Was the data involved in the breach recovered?
    a. If so, specify what and when it was recovered and who has the media now.

    b. If not recovered, explain the impact or potential misuse of the data.

    c. If not recovered, explain what is being done to find or recover the data.

8. What corrective action, mitigation, or notification is being considered at the department level?

9. What recommended action is suggested for consideration by the Privacy and Security Officer?

Was the P&S Officer contacted?: Date Contacted:

Report prepared by: **Date Prepared:**