

**MEMORANDUM
PLACER COUNTY HEALTH AND HUMAN SERVICES
Administration**

TO: Honorable Board of Supervisors

FROM: Jeffrey S. Brown, M.P.H., M.S.W., Director of Health and Human Services
Doreen Drake, Placer County HIPAA Privacy Officer

Kathy Buchanan, Deputy Director of Information Technology, Administrative Services Dept.
Rick Branicki, Placer County HIPAA Security Officer

DATE: October 7, 2014

SUBJECT: Approval of Health Insurance Portability Accountability Act Privacy and Security Policies

ACTION REQUESTED:

1. Adopt a Resolution approving Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Policies, and authorizing the Director of Health and Human Services to approve changes to these policies subject to reauthorization by the Board not less than every 5 years.

BACKGROUND:

In June 2009, this Board passed a resolution declaring the County of Placer to be a Hybrid Entity for purposes of compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH). The Hybrid Entity designation limits the applicability of HIPAA to only those County departments or programs that are appropriate under HIPAA standards. Placer County departments and programs not covered by HIPAA are still subject to other confidentiality laws regarding their handling and protection of medical and personal information. The resolution also delegated to the HHS Director, in conjunction with the HIPAA privacy and security officers, the authority to identify those County departments and programs that are part of the County Hybrid Entity. HHS developed the necessary policies and procedures to implement these laws.

The current County departments and programs that have been identified as being covered entities under the County's Hybrid Entity Designation are all found within the Department of Health and Human Services (HHS). They are: Medical Clinic; Public Health – Laboratory, California Children's Services (direct care components), HIV program; Adult System of Care - Mental Health Services, Substance Use Disorders Services, Managed Care Plan; Children's System of Care – Mental Health Services, Child Welfare Services (nursing and mental health components).

The current County departments and programs that have been identified as being business associate-like entities under the County's Hybrid Entity Designation are: Auditor-Controller; County Counsel; Administrative Services - Information Technology Division; HHS Administration; Public Health – California Children's Services (case management components), Child Health Disability and Prevention, Field Nursing program.

In 2013, the U.S. Department of Health and Human Services issued its final Omnibus Rule enhancing privacy protections, creating new patient rights, and strengthening enforcement under HIPAA and HITECH. These changes prompted modification of the County's privacy and security policies and procedures.

To ensure compliance with Federal and State laws and regulations related to HIPAA, HHS retained a consultant to review and update these policies, as well as to conduct a security risk assessment and evaluation of the County's existing HIPAA program. The results of the security risk assessment found Placer County to be among the most compliant organizations, requiring only nominal changes in existing protocols.

These updated policies have been reviewed and approved by County Counsel. HHS and Administrative Services/IT are requesting approval of these policies by the Board and authorization to make interim changes to these policies, with resubmission of any modifications of policies to the Board no less than every five years.

FISCAL IMPACT:

There is no impact to the County General Fund as a result of this action.

Attachment: Resolution with Policies

**Before the Board of Supervisors
County of Placer, State of California**

In the matter of:

Resolution No: _____

A Resolution approving HIPAA Privacy and Security Policies, and authorizing the Director of Health and Human Services to approve policy changes.

Ord. No.: _____

First Reading: _____

The following Resolution was duly passed by the Board of Supervisors of the County of Placer at a regular meeting held _____ by the following vote on roll call:

Ayes:

Noes:

Absent:

Signed and approved by me after its passage.

Chair, Board of Supervisors

Attest: _____
Clerk of said Board

WHEREAS, In June 2009, the Placer County Board of Supervisors adopted a resolution declaring the County of Placer to be a Hybrid Entity for purposes of compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The resolution also delegated to the HHS Director, in conjunction with the HIPAA privacy and security officers, the authority to identify those County departments and programs that are part of the HIPAA Hybrid Entity. The Board also adopted a companion resolution delegating to the HHS Director the authority to appoint the HIPAA privacy officer and security officer.

WHEREAS, as a result of changes to Federal law the Placer County HIPAA privacy officer and security officer have updated Placer County's HIPAA policies.

NOW, THEREFORE, BE IT RESOLVED, the Board of Supervisors of the County of Placer, State of California, hereby approves the HIPAA Privacy and Security Policies contained in Attachments 1 and 2 of this Resolution;

BE IT FURTHER RESOLVED that the Board of Supervisors hereby authorizes the Director of Health and Human Services, in conjunction with the Placer County HIPAA privacy officer and security officer, to create HIPAA forms and procedures and to modify adopted HIPAA policies or create new HIPAA policies with any such policy changes to be submitted to the Board of Supervisors for re-authorization not less than every five years.

Attachment 1: Privacy Policies (Numbers 001 - 022)
Attachment 2: Security Policies (Numbers 01 - 16)

283



HIPAA SECURITY POLICIES

COUNTY OF PLACER

Policy Title:	<i>Assigned Security Responsibility and Definitions</i>		
Policy Number:	01	Version:	1.0
Approved By:	HIPAA Security Officer/ Placer County Board of Supervisors		
Effective Date:			
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or Hybrid Business Associate-like entity.		

Purpose:

At all times the County of Placer shall have one individual identified and assigned to HIPAA Security Responsibility.

Definitions Applicable to All HIPAA Security Policies:

Business Associate – With respect to Placer County, a person who on behalf of the County, but other than in the capacity of a County employee, performs or assists in the performance of a function or activity involving the use or disclosure of PHI, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing benefit management, practice management, and re-pricing; or any other function or activity regulated by Federal privacy regulations; or provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for Placer County, where the service involves disclosure of PHI from the County, or from another Business Associate of the County.

Business Associate-like Entity -- A Placer County department, division, office, program or employee of the County of Placer which has been formally designated as being a Placer County HIPAA hybrid Business Associate-like entity.

Covered Component – an entity under the HIPAA Privacy Rule that must comply with the Rule's requirements for safeguarding the privacy of protected health information, and as formally designated as being a covered entity under the Placer County HIPAA hybrid covered entity designation.

HHS – The Health and Human Services Department of Placer County.

284



HIPAA SECURITY POLICIES

COUNTY OF PLACER

HIPAA – (The Health Insurance Portability and Accountability Act of 1996) A federal law that protects health insurance coverage for individuals and requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.

IT – The Information Technology Division of Placer County’s Administrative Services Department.

PHI – (Protected Health Information) Information that is under the control of a “covered entity” or its Business Associates that relates to the past, present, or future condition, either physical or mental, of an individual, identifying the individual or having enough information in it so that a reasonably prudent person would be able to identify the individual.

PII – (Personally Identifiable Information) personal information that can identify an individual, combined with one or more data elements such as a Social Security number, driver’s license ID (or non-driver ID card), financial information such as bank account or credit/debit card information numbers with access codes, or data elements that allow access to online accounts.

Workforce Members -- Placer County HIPAA Hybrid Covered Component employees, volunteers, or interns, and/or Hybrid Business Associate-like entity employees, volunteers, or interns, who have access to PHI.

Policy:

1. **General**

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, but are not limited to:

- 1.1. Ensure that the necessary and appropriate **HIPAA** related policies are developed and implemented to safeguard the integrity, confidentiality, and availability of electronic **PHI** within the covered entity.
- 1.2. Ensure the necessary infrastructure of personnel, procedures, and systems is in place (this policy does not apply to uses or disclosures):
 - 1.2.1. To develop and implement the necessary **HIPAA** related policies;

285



HIPAA SECURITY POLICIES

COUNTY OF PLACER

-
- 1.2.2. To monitor, audit and review compliance with all **HIPAA** related policies;
 - 1.2.3. To provide a mechanism for reporting incidents and **HIPAA** security violations.
 - 1.3. Act as a spokesperson and single point of contact for Placer County in all issues related to **HIPAA** security.
 - 1.4. Act as the lead individual responsible for investigating breaches in electronic **PHI**, and responding to complaints and investigations from State and Federal authorities regarding such breaches.
 - 1.5. Ensure compliance with applicable federal, state and local laws pertaining to security of data.
 - 1.6. Confirming that workforce members receive proper security training on an ongoing basis.
 2. The **HIPAA** Security Officer is appointed by the Director of **HHS**. For purposes of **HIPAA** security, this officer reports to the **HHS** Director or his/her designee.

Reference(s):

- 45 *CFR* Parts 164.308 (a) (2)

Contact(s):

- **HIPAA** Security Officer (see main internal **HHS** web page for contact information)

286



HIPAA SECURITY POLICIES

COUNTY OF PLACER

Policy Title:	<i>Risk Management Strategy- Electronic PHI</i>		
Policy Number:	02	Version:	1.0
Approved By:	HIPAA Security Officer/ Placer County Board of Supervisors		
Effective Date:	October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or Hybrid Business Associate-like entity.		

Purpose:

HHS will implement a risk management strategy to evaluate current security measures regarding electronic protected health information and implement measures to continuously monitor and improve security of electronic protected health information.

Definition:

See *HIPAA Security Policy 01, Assigned Responsibility and Definitions* for definitions applicable to all policies.

Risk Assessment - the determination of the quantitative or qualitative value of risk related to a recognized threat (also called vulnerability).

Risk Analysis - is a technique used to identify and assess factors that may jeopardize the success of a program or the achievement of a goal.

Policy:

1. Logical processes and technical controls will be implemented to reduce the risks to electronic PHI to a reasonable and appropriate level.
2. A full or partial network **Risk Assessment** and **Risk Analysis** will be completed annually as appropriately defined or may be required when:
 - 2.1. New threats or risks are identified that can impact PHI.
 - 2.2. A security incident occurs that impacts the PHI.
 - 2.3. A breach of unsecured protected health information occurs as defined in the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH).
 - 2.4. Changes to Placer County information security requirements or responsibilities that impact PHI.
 - 2.5. Changes to Placer County's organizational or technical infrastructure that impacts the protected information.

287



HIPAA SECURITY POLICIES

COUNTY OF PLACER

3. The analysis of the assessment will be submitted to the appropriate **HHS** Executive Management team and the Director of **HHS**.
4. The Executive Management team will review the findings, and submit a report to the Director of **HHS** with recommendations regarding what actions need to be taken.
5. Future **Risk Assessments** and **Risk Analysis** as defined in item 2 above will evaluate whether or not the recommended actions were implemented and if they were effective.

Reference(s):

- *45 CFR Parts 164.308 (a) (1) (ii) (B)*

Contact(s):

- **HIPAA** Security Officer (see main internal **HHS** web page for contact information)



HIPAA SECURITY POLICIES COUNTY OF PLACER

Policy Title:	<i>Sanctions</i>		
Policy Number:	03	Version:	1.0
Approved By:	HIPAA Security Officer/ Placer County Board of Supervisors		
Effective Date:	October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or Hybrid Business Associate-like entity.		

Purpose:

To specify enforcement, sanction, penalty, and disciplinary actions that may result from violation of County policies regarding the security of an individual's **PHI**.

Definition:

See *HIPAA Security Policy 01, Assigned Responsibility and Definitions* for definitions applicable to all policies.

Policy:

Placer County will apply appropriate sanctions against **workforce members** who fail to comply with the security policies and procedures of the County's covered entity as described in the policy section of the Placer County *HIPAA Privacy Policy 014, Enforcement, Sanctions, and Penalties for Violations of Individual Privacy*.

Reference(s):

- 45 CFR 164.308 (a) (1)(ii)(C)
- Placer County *HIPAA Policy 014*

Contact(s):

- HIPAA Security Officer (see main internal HHS web page for contact information)



HIPAA SECURITY POLICIES

COUNTY OF PLACER

Policy Title:	<i>Workforce Security</i>		
Policy Number:	04	Version:	1.0
Approved By:	HIPAA Security Officer/ Placer County Board of Supervisors		
Effective Date:	October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or Hybrid Business Associate-like entity.		

Purpose:

The purpose of this policy is to establish rules for authorizing access to the computing network, applications, workstations, and to areas where **PHI** is accessible. **Workforce members** shall have authorization when working with **PHI** or when working in locations where it resides. Workforce security includes ensuring that only **workforce members** who require access to **PHI** for work related activities shall be granted access and that when work activities no longer require access, authorization shall be terminated.

Definition:

See *HIPAA Security Policy 01, Assigned Responsibility and Definitions* for definitions applicable to all policies.

Policy:

1. Management and Access Control

- 1.1. Only the workforce member's supervisor or manager may grant access to the County's **PHI** information systems.
- 1.2. 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 resources.
- 1.3. Any individual whose access is revoked or suspended may be subject to disciplinary action or other appropriate corrective measures as stated in *HIPAA Policy 014, "Enforcement, Sanctions, and Penalties for Violations of Individual Privacy."*

2. Minimum Necessary Access

- 2.1. Each covered component shall ensure that only **workforce members** who require access to **PHI** are granted access.



HIPAA SECURITY POLICIES

COUNTY OF PLACER

- 2.2. Each supervisor or manager is responsible for ensuring that the access to **PHI** granted to each of his/her subordinates is the minimum necessary access required for each subordinate's job role and responsibilities.
- 2.3. If the user no longer requires access, it is the supervisor or manager's responsibility to complete the necessary process to terminate access.
3. **Granting Access to PHI**
 - 3.1. User access accounts can only be assigned with management approval or by an appropriate designee.
 - 3.2. Managers are responsible for requesting the appropriate level of computer access for staff to perform their job function.
 - 3.3. All requests regarding user access accounts for **workforce members** are to be communicated in written form, either on paper or electronically, to the appropriate system administrator by completing the required forms for covered components.
 - 3.4. System administrators are required to process only those requests that have been authorized by managers or their designees.
 - 3.5. A written record of the authorized request is to be retained by the system administrator for a minimum one (1) year.
 - 3.6. Before access is granted in any of the various systems or applications that contain **PHI**, **workforce members** shall be trained to a minimum standard including:
 - 3.6.1. General HIPAA training as provided by the County.
 - 3.6.2. The **workforce member** will sign an acknowledgement that he/she has received and understands the HIPAA training.
 - 3.6.3. Proper uses and disclosures of the **PHI** stored in the systems and applications.
 - 3.6.4. How to properly log on and log off the systems and applications.
 - 3.6.5. Protocols for correcting user errors.
 - 3.6.6. How to contact the help desk when **PHI** may have been altered or destroyed.
 - 3.6.7. How to report a potential or actual security breach.
 - 3.7. Prior to being issued a user access account to access **PHI**, each workforce member shall sign the *Placer County Acknowledgement of Information Security Responsibility* form before access is granted to the County network or any application that contains **PHI**.
4. **Granting Access In an Emergency**
 - 4.1. If management grants emergency access, she/he shall review the impact of emergency access and document the event within 72 hours of it being granted.
 - 4.2. After the emergency event is over, the user access shall be removed or the **workforce member** shall complete normal requirements for being granted access.



HIPAA SECURITY POLICIES

COUNTY OF PLACER

5. Granting Emergency Access to an Existing User Access Account

5.1. 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:

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

5.1.2. The **workforce member** is out for a prolonged period.

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

5.1.4. Manager/Supervisor needs immediate access to data on a **workforce member's** computer in order to provide patient treatment.

6. Termination of Access

6.1. The department manager/supervisor is responsible for terminating a **workforce member's** access to **PHI** in these circumstances:

6.1.1. When management has evidence or reason to believe that the individual is using information systems or resources in a manner inconsistent with the HIPAA Security policies.

6.1.2. When the **workforce member** or management has evidence or reason to believe the user's password has been compromised.

6.1.3. When the employee resigns, is terminated, is suspended, retires, or has not been in attendance and therefore is assumed to have resigned.

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

7. Modifications to the Workforce member's Access

7.1. When the **workforce member** transfers to another program or changes role within the same program within the County's covered component:

7.1.1. The **workforce member's** new supervisor or manager is responsible for evaluating the member's current access and for requesting new access to **PHI** commensurate with the **workforce member's** new job description.

7.2. When the **workforce member** transfers to another program or department outside the County's covered entity:

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

7.2.2. The **workforce member's** new supervisor or manager is responsible for requesting access to **PHI** commensurate with the **workforce member's** new job description.

8. Compliance for Access



HIPAA SECURITY POLICIES

COUNTY OF PLACER

8.1. In order to ensure that **workforce members** only have access to **PHI** when it is required for their job duties, the following actions shall be implemented by all covered components:

8.1.1. Every new user access account that has not been used after 90 consecutive days since creation shall be investigated to determine if the **workforce member** still requires access to **PHI**.

8.1.2. At the request of **HHS** management, **IT** shall send to **HHS** division managers:

8.1.2.1. A list of all **workforce members** for all applications.

8.1.2.2. A list of **workforce members** and their access rights for all shared folders that contain **PHI**.

8.1.2.3. A list of all virtual private network **workforce members**.

8.1.3. The division manager in conjunction with his/her management team will evaluate the workforce to determine who needs continued access to **PHI** and notify **IT** of those **workforce members** who no longer need access to **PHI** or their access modified.

9. **IT Responsibilities**

9.1. Immediately upon written notification from the program manager or division management, the **IT** staff will add access, terminate access, or modify access to programs and applications that contain **PHI**.

9.2. An annual report shall be submitted to the County Privacy officer from **IT** documenting the number of **workforce members** granted access, denied access, and had access modified to **PHI** applications and programs.

Reference(s):

- 45 CFR 164.308 (a) (3)
- 45 CFR 164.308 (a) (4)
- 45 CFR 164.308 (a) (5)

Contact(s):

- HIPAA Security Officer (see main internal **HHS** web page for contact information)



HIPAA SECURITY POLICIES

COUNTY OF PLACER

Policy Title:	<i>Information Security Audit Controls and System Activity Review</i>		
Policy Number:	05	Version:	1.0
Approved By:	HIPAA Security Officer/ Placer County Board of Supervisors		
Effective Date:	October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or Hybrid Business Associate-like entity.		

Purpose:

This policy details the requirements of **HHS** for **IT** audit controls, and monitoring and review of system activity to safeguard systems that contain Confidential Information, such as **PHI** and **PII**. The policy complies with HIPAA Security Regulations, Technical Safeguards, 45 C.F.R 164.312(b). In addition, this policy supports the *Information Security Breach Notification*, the *Health Information Technology for Economic and Clinical Health Act (HITECH)* and other state laws that require safeguards in systems that contain confidential information.

Definition:

See *HIPAA Security Policy 01, Assigned Responsibility and Definitions* for definitions applicable to all policies.

Policy:

1. General

1.1. Placer County will implement, where technically feasible, appropriate hardware, software or procedural mechanisms on all systems containing Confidential Information, and will review the logs created by these audit mechanisms on an ongoing basis.

2. Requirements and Responsibilities

2.1. **HHS** records and reviews significant activity on all of its systems that contain Confidential Information.

2.2. **IT** will conduct a risk analysis, to identify and define what constitutes “significant or unusual activity” on any information system, repository or conduit that contains Confidential Information.

2.3. **IT** must implement appropriate hardware, software and procedural mechanisms on any information system, repository or conduit that contains Confidential



HIPAA SECURITY POLICIES

COUNTY OF PLACER

Information to log all access. At a minimum, such logs should contain the following information:

- 2.3.1. Date and time of activity.
- 2.3.2. Origin of activity (e.g., I/P address, workstation ID).
- 2.3.3. Identification of individual performing activity.
- 2.3.4. Description of activity (view, modification, deletion of data, etc.).
- 2.3.5. Identity of the individual whose Confidential Information was accessed.
- 2.4. In addition to logging authorized access of Confidential Information, **IT** will also monitor and log its systems to provide additional information for detecting and analyzing suspicious activity by logging, where possible, information such as:
 - 2.4.1. Use of software programs or utilities (e.g. system logs).
 - 2.4.2. Use of privileged accounts.
 - 2.4.3. Identification of administrator activity (e.g. account or access creation, modification, or deletion).
 - 2.4.4. System start-up or shut-down.
 - 2.4.5. Failed authentication attempts.
- 2.5. The appropriate level and type of auditing that is required should be determined by a risk analysis which takes into consideration the following factors:
 - 2.5.1. The merit or sensitivity of the information on the systems.
 - 2.5.2. The importance of the applications operating on the information systems.
 - 2.5.3. The degree to which the information systems are connected to other systems and the degree to which that connection poses a risk to the system.
- 2.6. **IT** must implement and document a process for regular review of all audit logs. This process may be contained in-house or an outside party may be engaged to perform log analysis and correlation. The documented procedure must identify:
 - 2.6.1. Workforce members, or the third party responsible for reviewing logs.
 - 2.6.2. Specific logs which are included in the review.
 - 2.6.3. Frequency of the review (weekly, daily, etc.).
 - 2.6.4. Response to incidents detected by log review.
 - 2.6.5. Audit record retention period.
- 2.7. **IT** workforce members cannot be responsible for reviewing audit logs that pertain to their system activities, and the administrator of a particular system may not be responsible for auditing the logs for that same system.
- 2.8. Audit logs must be stored in such a way that they cannot be deleted or modified in any way.

Reference(s):



HIPAA SECURITY POLICIES

COUNTY OF PLACER

- 45 C.F.R 164.312 (b)

Contact(s):

- HIPAA Security Officer (see main internal HHS web page for contact information)



HIPAA SECURITY POLICIES

COUNTY OF PLACER

Policy Title:	<i>Contingency Planning and Data Backups</i>		
Policy Number:	06	Version:	1.0
Approved By:	HIPAA Security Officer/ Placer County Board of Supervisors		
Effective Date:	October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or Hybrid Business Associate-like entity.		

Purpose:

This policy details the requirements of a **Covered Component** to have contingency plans in place for the continuity of operations during a natural or man-made disaster or emergency, or during times when there is a loss of operational functionality due to technical issues such as equipment or software failures. It also specifies requirements for the classification and backup of the application and data.

Definition:

See *HIPAA Security Policy 01, Assigned Responsibility and Definitions* for definitions applicable to all policies.

Policy:

1. General

- 1.1. Each **Covered Component** shall develop plans and procedures for continuing business in the event of an emergency, disaster, or other occurrence (fire, vandalism, system failure, etc.) which results in the failure of the system that contains **PHI**. Such plans will include:
 - 1.1.1. Applications and data criticality analysis.
 - 1.1.2. Data backup plans.
 - 1.1.3. Disaster Recovery plan.
 - 1.1.4. Emergency mode of operation plan.
- 1.2. Each **Covered Component** shall evaluate and update their plans as business needs and technology requirements change.

2. Applications and data Criticality Analysis

- 2.1. Each **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 of Operation Plan.



HIPAA SECURITY POLICIES

COUNTY OF PLACER

- 2.2. Each **Covered Component** shall identify critical business functions, define impact scenarios, and determine resources needed to recover from each impact.
- 2.3. The assessment of data and applications criticality shall be conducted periodically to ensure that appropriate procedures are in place for data and applications at each level of risk.
3. **Data Backup Plan**
 - 3.1. All **PHI** shall be stored on network servers in order for it to be automatically backed up by the system.
 - 3.2. **PHI** shall not be saved on local drives of personal computers.
 - 3.3. **PHI** stored on portable media devices shall be saved to the network to ensure backup of **PHI** data.
 - 3.4. Working in cooperation with IT where necessary, each **Covered Component** shall establish and implement a Data Backup Plan pursuant to which it would create and maintain retrievable exact copies of **PHI**.
 - 3.5. The Data Backup Plan shall apply to all files that contain **PHI**.
 - 3.6. Each **Covered Component** shall submit its Data Backup Plan to the County HIPAA County Privacy Officer.
 - 3.7. **IT** shall conduct daily backups of user-level and system level information and store the backup information in a secure location. At a minimum, a weekly backup shall be stored offsite.
 - 3.8. The Data Backup Plan shall require that media used for backing up **PHI** be stored in a physically secure environment.
 - 3.9. **HHS** and **IT** must take reasonable steps to ensure that all electronic data that is backed up in connection with movement of equipment into, out of, or within its facilities can be recovered following a disaster or other emergency, or a failure of the equipment during movement.
 - 3.10. **HHS** and **IT** will store backup copies of data and its records of the backup copies and restoration procedures in a secure remote location, within sufficient distance from Placer County's facilities to allow for prompt retrieval in the event of a disaster or other emergency, or a failure of the equipment during movement.
 - 3.11. **HHS** and **IT** must ensure that all off-site third party backup storage facility and transportation companies enter into Business Associate Agreements with Placer County, and require that each storage facility or transportation company implement appropriate administrative, technical and physical safeguards to ensure the confidentiality of the data.
 - 3.12. **IT** will make the backup copies of data stored at the remote location accessible only to authorized workforce members for retrieval when needed in the event of a disaster or other emergency, or a failure of the equipment, during movement.



HIPAA SECURITY POLICIES

COUNTY OF PLACER

3.13. **IT** will test the backup and restoration procedures on a regular basis. Placer County will take reasonable steps to ensure that the procedures are effective and can be completed within a reasonable amount of time.

4. **Disaster Recovery Plan**

4.1. To ensure that each **Covered Component** can recover from the loss of data due to an emergency or disaster such as a fire, vandalism, terrorism, system failure, or natural disaster effecting systems containing **PHI**, each **Covered Component** shall establish and implement a Disaster Recovery Plan pursuant to which it can restore or recover any loss of **PHI** and the systems needed to make that **PHI** available in a timely manner.

4.2. Each **Covered Component** will work with **IT** to develop and implement a Disaster Recovery Plan for automated systems effecting **PHI**.

4.3. Each **Covered Component** is directly responsible for the development and implementation of manual functional processes while automated systems are not available during a disaster.

4.4. The Disaster Recovery Plan will identify roles and responsibilities of **workforce** members, and all appropriate **workforce members** will receive regular training and awareness on the Disaster Recovery Plan.

4.5. These plans shall be tested and a copy sent to the HIPAA Privacy Officer. A copy of the plans will also be kept off-site as described in item 3.10 above.

5. **Emergency Mode Operation Plan**

5.1. Emergency mode operation involves those critical business processes that shall occur to protect the security of electronic **PHI** during and immediately after a crisis, and the commitment to take reasonable steps to ensure that in the event of a disaster, **workforce members** can enter the facilities to take necessary action. **IT** will work with **Covered Components** to develop such a plan.

5.2. Based on its Disaster Recovery Plan, **HHS** and **IT** will develop, implement and periodically review a documented procedure to allow authorized **workforce members** access to Placer County's facilities to support restoration of lost data. Placer County defines **workforce members**' roles in its Disaster Recovery Plan, and addresses all facilities, **PHI** systems and electronic media involved. Placer County's Disaster Recovery Plan defines how the actions taken by such workforce members are tracked and logged, and how unauthorized accesses can be detected.

5.3. In the event of a disaster or other emergency, only authorized **HHS** and **IT workforce members** are permitted to administer or modify processes and controls that protect the security of **PHI**.



HIPAA SECURITY POLICIES

COUNTY OF PLACER

Reference(s):

- 45 CFR 164.308 (a) (7)
- 45 CFR 164.310 (a) (2) (i)
- 45 CFR 164.310 (a) (2) (iv)

Contact(s):

- HIPAA Security Officer (see main internal HHS web page for contact information)



HIPAA SECURITY POLICIES

COUNTY OF PLACER

Policy Title:	<i>Incident Response</i>		
Policy Number:	07	Version:	1.0
Approved By:	HIPAA Security Officer/ Placer County Board of Supervisors		
Effective Date:	October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or Hybrid Business Associate-like entity.		

Purpose:

The purpose of this policy is to define the requirements to respond to and report 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.

Definition:

See *HIPAA Security Policy 01, Assigned Responsibility and Definitions* for definitions applicable to all policies.

Policy:

1. Reporting

- 1.1. Incidents that shall be reported include, but are not limited to:
 - 1.1.1. Virus, worms, or other malicious code attacks that activate on County systems and devices.
 - 1.1.2. Network system intrusions.
 - 1.1.3. Persistent intrusion attempts from a particular entity.
 - 1.1.4. Unauthorized access to **PHI**, a **PHI**-based system, or a **PHI**-based network.
 - 1.1.5. **PHI** data loss due to disaster, failure, error, theft.
 - 1.1.6. Loss of electronic media that contains **PHI**.
 - 1.1.7. Loss of integrity of **PHI**.
 - 1.1.8. Unauthorized person found in a covered components facility.
- 1.2. The IT Help Desk (Customer Services Center) shall be notified immediately of any suspected or real security incident.

2. Response and Resolution



HIPAA SECURITY POLICIES

COUNTY OF PLACER

- 2.1. The IT Help Desk shall report the incident to the Security Officer and to the Privacy Officer, and the IT Help Desk will assign the incident to the IT Security Services team.
 - 2.2. The Security Officer will:
 - 2.2.1. Investigate the breach.
 - 2.2.2. Determine the extent of the loss of **PHI**.
 - 2.2.3. Develop a plan of corrective action to mitigate the problem and stem further loss of **PHI**.
 - 2.2.4. Implement the plan of corrective action.
 - 2.3. Depending on the nature and extent of the breach as it relates to the compromise of **PHI** or **PII**, these additional actions are required:
 - 2.3.1. The **HHS** Director, the Director of Administrative Services, the **IT** Director, County Counsel and Risk Management will be notified.
 - 2.3.2. The appropriate local, state, and federal agencies will be contacted.
 - 2.3.3. All media communication will be coordinated and approved by the **HHS** director.
3. **Recording of Incidents**
- 3.1. All HIPAA security related incidents and their outcomes shall be recorded by **IT** and reported immediately to the HIPAA Privacy Officer.
 - 3.2. This report shall be used in the Annual Risk Analysis Completed by the HIPAA Security officer.
 - 3.3. The lessons learned from the breach including how it occurred and the strategies used to mitigate further loss of **PHI** will be incorporated in future HIPAA Security Training.

Reference(s):

- 45 CFR 164.308(a)(6)

Contact(s):

- HIPAA Security Officer (see main internal HHS web page for contact information)



HIPAA SECURITY POLICIES

COUNTY OF PLACER

Policy Title:	<i>Business Associate Contracts and Other Arrangements</i>		
Policy Number:	08	Version:	1.0
Approved By:	HIPAA Security Officer/ Placer County Board of Supervisors		
Effective Date:	October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or Hybrid Business Associate-like entity.		

Purpose:

The intent of this policy is to establish the requirement for procedures which determine which contractual and business relationships are considered "Business Associates" as defined by **HIPAA**. In addition this policy establishes the requirement to track designated Business associates and provide procedures to follow up on complaints about the Business Associate.

Definition:

See *HIPAA Security Policy 01, Assigned Responsibility and Definitions* for definitions applicable to all policies.

Policy:

1. Placer County will develop and maintain procedures to:
 - 1.1. Determine which contractual and business relationships are considered **Business Associates**.
 - 1.2. Track **Business Associates**.
 - 1.3. Follow up on complaints received regarding **Business Associates**.

Reference(s):

- 45 CFR 164.308(b)(1)
- *HIPAA Privacy Policy 012 "Business Associate Relationships"*

Contact(s):

- HIPAA Security Officer (see main internal HHS web page for contact information)



HIPAA SECURITY POLICIES

COUNTY OF PLACER

Policy Title:	<i>Security Malware Protections</i>		
Policy Number:	09	Version:	1.0
Approved By:	HIPAA Security Officer/ Placer County Board of Supervisors		
Effective Date:	October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or Hybrid Business Associate-like entity.		

Purpose:

The purpose of this policy is to establish criteria for protections to guard against, detect, and report malicious software (Malware). Malware software includes, but is not limited to, viruses, worms, and Trojans.

Definition:

See *HIPAA Security Policy 01, Assigned Responsibility and Definitions* for definitions applicable to all policies.

Malware – (Malicious Software) software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of computer program code, scripts, active content, and other software. Malware is a general term used to refer to a variety of forms of hostile or intrusive software. Malware includes computer viruses (including Worms and Trojan Horses), Ransomware, Spyware, Adware, Scareware and other malicious programs.

Policy:

1. **Malware Protections**

- 1.1. **Covered Components** shall ensure all computers (owned, leased, and/or operated by the covered components) install, implement and maintain anti-**malware** (anti-virus) software. All workstations shall be configured to activate and update anti-**malware** software automatically each time the user logs on the County network.
- 1.2. **IT** will set up laptops or where technically feasible, tablets and mobile devices, so they automatically load anti-**malware** updates when they are connected to the County network.
- 1.3. **Workforce members** who utilize laptops, or where technically feasible, tablets and mobile devices, to log on to the County network shall work with **IT** to ensure all anti-**malware** updates are received.



HIPAA SECURITY POLICIES

COUNTY OF PLACER

- 1.4. **Workforce members** are not to disable automatic **malware** scanning features.
- 1.5. All non-County computing devices that directly access the County's Enterprise Network and information systems assets shall have anti-**malware** software installed and operational, and remain current with updates.
- 1.6. In the event that **malware** has been identified on a server or workstation, that equipment shall be disconnected from the network until it has been appropriately cleaned.
- 1.7. With the full cooperation of the **Covered Component**, any **malware** detected and found to have been activated on a **Covered Component's** computer will be fully investigated by **IT** to determine if **PHI or PII** has been compromised. In the case of **PHI or PII** compromise, requirements described in *HIPAA Security Policy 07, Incident Response* will apply.
- 1.8. For the purposes of protecting data and preventing the spread of malware:
 - 1.8.1. **IT** workers will be provided security training which includes virus protection issues and current malicious software trends.
 - 1.8.2. General **workforce members** will receive Security training that includes up to date information on viruses, worms, etc. and what to do when malware is discovered on their computer.
 - 1.8.3. **IT** will maintain back-ups of **PHI** data files.

Reference(s):

- 45 CFR 164.308(a)(5)(ii)(B)

Contact(s):

- HIPAA Security Officer (see main internal HHS web page for contact information)



HIPAA SECURITY POLICIES

COUNTY OF PLACER

Policy Title:	<i>Security Awareness Training</i>		
Policy Number:	10	Version:	1.0
Approved By:	HIPAA Security Officer/ Placer County Board of Supervisors		
Effective Date:	October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or Hybrid Business Associate-like entity.		

Purpose:

The purpose of this policy is to define the requirements for Security Awareness Training for Placer County **workforce members** who have access to **PHI**. Placer County **workforce members** will be provided with training to enable them to appropriately protect Placer County's **PHI**. New Placer County **workforce members** will receive the appropriate security training prior to being provided access to Placer County's **PHI**. Placer County will make business associates aware of Placer County's security policies and procedures when and if appropriate. Additionally, third parties who have access to Placer County's **PHI** will also be informed of Placer County's security policies and procedures when and if appropriate and will be required to execute an Acknowledgment form indicating that they have received certain policies and will abide by them.

Documentation will be maintained regarding the individuals who have undergone training.

Definition:

See *HIPAA Security Policy 01, Assigned Responsibility and Definitions* for definitions applicable to all policies.

Policy:

1. Security Awareness Training

1.1. Placer County will provide security awareness training to Placer County **workforce members** who have access to **PHI** to enable them to appropriately protect Placer County's **PHI**.

1.1.1. In accordance with Placer County's breach notification policies and procedures, Placer County will train and remind its **workforce members** of the proper procedures for reporting a security incident or a breach.



HIPAA SECURITY POLICIES

COUNTY OF PLACER

- 1.2. New Placer County **workforce members** will receive the appropriate security training prior to being provided access to Placer County's **PHI**.
- 1.3. Placer County will make **Business Associates** aware of Placer County's security policies and procedures when and if appropriate.
- 1.4. Third parties who have access to Placer County's **PHI** will also be informed of Placer County's security policies and procedures when and if appropriate and will be required to execute an Acknowledgment form indicating that they have received certain policies and will abide by them.
- 1.5. Documentation will be maintained regarding the individuals who have undergone training.

Reference(s):

- 45 CFR 164.308(a)(5)(i)
- 45 CFR 164.308(a)(5)(ii)(A)

Contact(s):

- HIPAA Security Officer (see main internal HHS web page for contact information)



HIPAA SECURITY POLICIES

COUNTY OF PLACER

Policy Title:	<i>Facility Access Controls</i>		
Policy Number:	11	Version:	1.0
Approved By:	HIPAA Security Officer/ Placer County Board of Supervisors		
Effective Date:	October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or Hybrid Business Associate-like entity.		

Purpose:

The purpose of this policy is to establish protocols for securing facilities that contain **PHI**. The County of Placer shall reasonably safeguard electronic **PHI** from any intentional or unintentional use or disclosure. The county shall protect its facilities where **PHI** can be accessed.

Definition:

See *HIPAA Security Policy 01, Assigned Responsibility and Definitions* for definitions applicable to all policies.

Policy:

1. Facility Security Plan

- 1.1. The County will safeguard the facilities of its covered components and the equipment therein from unauthorized physical access, tampering, and theft.
- 1.2. The Security Officer or delegate will conduct an annual audit of **Covered Component** facilities to ensure **PHI** safeguards and submit a report to the County Privacy officer.

2. Visitor Access Control

- 2.1. In facilities in which **PHI** is available, all visitors will be escorted and monitored.
- 2.2. Each facility will implement procedures that govern visitor access controls. These procedures may vary depending on the facilities structure, type of visitors, and where the **PHI** is accessible.

3. Metal/hard Keys

- 3.1. Facilities that use metal keys will change the appropriate key locks when keys are lost or stolen and there is a perceived risk that the facility is vulnerable to unauthorized entry.



HIPAA SECURITY POLICIES

COUNTY OF PLACER

- 3.2. Managers/supervisors will collect the keys of **workforce members** upon termination or retirement from employment.
4. **Keypads/Cipher Locks**
 - 4.1. The Facility Manager will change the codes on keypads/cipher locks at least every six months in order to ensure security of staff, property, and the confidentiality of patient information.
 - 4.2. In addition, the facility will have:
 - 4.2.1. Clearance based on programmatic need, special mandated security requirements and **workforce member** security.
 - 4.2.2. A mechanism to track which **workforce members** are provided access.
5. **Security Access Cards**
 - 5.1. Some facilities have security access cards to gain entry into the facility. These facilities will include a card management system and a monitoring system to ensure the appropriate use of security access cards.
 - 5.2. There will be a back-up system in case of system failure and a system for disabling cards when a **workforce member** leaves County employment.
6. **Network Closet(s)**
 - 6.1. Every server room will be locked whenever the room is unoccupied or not in use.
 - 6.2. **Covered Components** will document who has access to each server room and periodically change the locking mechanism to the server rooms.
7. **Contingency Operations**
 - 7.1. Each facility will have emergency access procedures in place that allow facility access when facility access is necessary after business hours by persons who do not currently have access to the facility, for access to data as well as to support restoration of lost data. This includes:
 - 7.1.1. A primary contact person.
 - 7.1.2. A back-up person if the primary contact is not available.
8. **Maintenance Records**
 - 8.1. Repairs or modifications to the physical building for each facility where **PHI** can be accessed will be logged and tracked.
 - 8.2. The repairs will be tracked by the County's Facility Services Department.
9. **Responsibilities**
 - 9.1. Managers/Supervisors
 - 9.1.1. Take appropriate corrective action against any person who knowingly violates the facility plan.
 - 9.1.2. Authorize clearances that are appropriate to the duties of each **workforce member**.



HIPAA SECURITY POLICIES

COUNTY OF PLACER

- 9.1.3. Notify the Facility Manager within one business day when a user no longer requires access to the facility.
- 9.1.4. Verify that each **workforce member** surrenders his/her card or key upon leaving employment.
- 9.2. Workforce Member
 - 9.2.1. Display their access/security card/name badge to demonstrate their authorization access to restricted areas.
 - 9.2.2. Immediately report lost or stolen cards, badges, or metal keys or keypad lock combinations.
 - 9.2.3. Surrender badge, access card, metal/hard keys upon leaving employment.
- 9.3. Facility Manager
 - 9.3.1. Request and track maintenance repairs.
 - 9.3.2. Establish mechanism for accessing the facility in an emergency.
 - 9.3.3. Track who has access to the facility.
 - 9.3.4. Change locks when indicated.
 - 9.3.5. Change keypad codes every 6 months.
 - 9.3.6. Provide annual training to staff on site security and emergency access.
 - 9.3.7. Disable access cards not used for 90 days.
 - 9.3.8. Audit access card use annually.
- 9.4. Security Officer
 - 9.4.1. Conduct annual audits of **Covered Component** facilities to ensure policies are being enforced.
 - 9.4.2. Ensure server room access is documented.
 - 9.4.3. Ensure server room locks are changed periodically where applicable.

Reference(s):

- 45 164.310(a)(1)

Contact(s):

- HIPAA Security Officer (see main internal HHS web page for contact information)



HIPAA SECURITY POLICIES

COUNTY OF PLACER

Policy Title:	<i>Workstation Use and Workstation Security</i>		
Policy Number:	12	Version:	1.0
Approved By:	HIPAA Security Officer/ Placer County Board of Supervisors		
Effective Date:	October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or Hybrid Business Associate-like entity.		

Purpose:

The purpose of this policy is to establish rules for securing workstations that access **PHI**. Since **PHI** is portable, this policy requires **workforce members** to protect **PHI** in all locations, including, but not limited to, homes, public areas, and client sites.

Definition:

See *HIPAA Security Policy 01, Assigned Responsibility and Definitions* for definitions applicable to all policies.

Policy:

1. Workstation Security

- 1.1. The County of Placer **workforce members** will ensure that observable confidential information is adequately shielded from unauthorized disclosure and unauthorized access on computer screens. Each **workforce member** will make every effort to ensure that confidential information on computer screens is not visible to unauthorized persons in the workplace.
- 1.2. **Workforce members** who work from home or other non-office sites shall take the necessary precautions to protect **PHI** from other persons who may have access to their home or other non-office site. These precautions include but are not limited to using:
 - 1.2.1. Password protection of their personal computer.
 - 1.2.2. Password protection of portable electronic storage devices such as CDs, memory sticks, flash memory devices, cellphones, tablets, etc. that contain **PHI**.
- 1.3. Workstations/devices that contain **PHI** will have a session-lock implemented when the computer is left idle.



HIPAA SECURITY POLICIES

COUNTY OF PLACER

1.3.1. The session-lock will be automatic after a specific time based on location and function.

1.3.2. The session shall be locked to disable access to the PC until the user enters their unique authenticator.

1.4. Portable computer/devices containing **PHI** will experience an automatic log off after 30 minutes of non-use where technically feasible.

2. Responsibilities

2.1. Managers/Supervisors

2.1.1. Take appropriate corrective action against any **workforce member** who knowingly violates the security of workstation use.

2.1.2. Ensure that **workforce members** set their computer to automatically lock when the computer is not in use. This will be done by **IT** on County computers.

2.1.3. Ensure that all **PHI** is not viewable by unauthorized persons at workstations in offices under their management.

2.1.4. Provide polarized screens or other computer security screen overlay devices that can shield **PHI** where applicable.

2.1.5. Ensure the placement of computers is out of visual range of persons other than the authorized user.

2.2. Workforce Member

2.2.1. Session lock the computer when left unattended.

2.2.2. Ensure that the computer is set to automatically lock the session when the computer is not in use. Notify **IT** if this is not occurring on County provided equipment.

2.2.3. Ensure that all **PHI** is not viewable by unauthorized persons.

2.2.4. When working at home or other non-office work sites, protect **PHI** from unauthorized access.

2.2.5. Clear **PHI** information from the screen when it is not actively in use.

2.3. IT

2.3.1. When installing new workstations for use with **PHI**, set the lock timer to lock the computer when left unattended after a specified period of time.

2.3.2. When installing new systems or applications for use with **PHI**, set the automatic logoff timer to terminate the session when the computer is left unattended after 30 minutes of non-use.

Reference(s):

- 45 CFR 164.310(b)



HIPAA SECURITY POLICIES

COUNTY OF PLACER

- 45CFR 164.310(c)

Contact(s):

- HIPAA Security Officer (see main internal HHS web page for contact information)



HIPAA SECURITY POLICIES

COUNTY OF PLACER

Policy Title:	<i>Device and Media Controls</i>		
Policy Number:	13	Version:	1.0
Approved By:	HIPAA Security Officer/ Placer County Board of Supervisors		
Effective Date:	October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or Hybrid Business Associate-like entity.		

Purpose:

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

Definition:

See *HIPAA Security Policy 01, Assigned Responsibility and Definitions* for definitions applicable to all policies.

Policy:

1. **Accountability and Controls of Computer Hardware**

- 1.1. Each **Covered Component** will protect all the hardware and electronic media that contain **PHI**, including, but not limited to, personal computers, laptops, cell phones, tablets, memory sticks, CDs, storage systems, backup tapes, and removable disks.
- 1.2. Each **Covered Component** is responsible to develop procedures that govern the receipt and removal of hardware and electronic media that contain **PHI** into and out of a facility, and movement of these items within the facility. Procedures shall include:
 - 1.2.1. A record of movements of hardware and electronic media.
 - 1.2.2. The name of the individual in possession of the hardware and electronic media.

2. **Portable Media Use**

- 2.1. **Workforce members** shall protect **PHI** when working from all other locations, including home, other County offices, or when working in the field.
- 2.2. In order to limit the amount of portable **PHI**, **workforce members** will limit the quantities of **PHI** on CDs, memory sticks, and other portable electronic storage devices to only what is necessary for the performance of their work assignment.



HIPAA SECURITY POLICIES

COUNTY OF PLACER

- 2.3. No portable device containing **PHI** shall be the original and only source of the data.
 - 2.3.1. The **PHI** data shall be stored on the County Enterprise Network so the data is copied for backup during the County's backup processes.
 - 2.3.2. When it is not feasible to store the **PHI** on the County Enterprise Network, a primary copy must be available on electronic media that can be retrieved in an emergency in accordance with *HIPAA Security Policy 06, Contingency Planning and Data Backups*.
- 2.4. All **workforce members** shall receive training (and sign an acknowledgment that they received the training) on securing **PHI** data on any portable device prior to using the device.
- 2.5. All **workforce members** shall receive written permission from their supervisor before removing **PHI** from their facility with the level and scope of permission determined by the **Covered Component**.
- 2.6. **Workforce members**, including management, will only use portable electronic storage devices approved by **IT**.
- 2.7. **Workforce members**, who work in the field, shall not leave devices containing **PHI** unlocked or visible in their vehicles or leave it unattended in a client's home or living facility.
- 2.8. If the device containing **PHI** is lost or stolen, **workforce members** are responsible to promptly contact their supervisor, the County's Security Officer, and the HIPAA Privacy officer within one business day.
3. **Disposal of PHI Devices**
 - 3.1. Before electronic media that contains **PHI** can be disposed of, the following actions shall be taken on computers used in the workforce, at home, or at remote sites. **IT** is available for consultation regarding the following:
 - 3.1.1. Hard drives shall be either wiped clean with an **IT** approved process or physically destroyed so that no media surface can be electronically read.
 - 3.1.2. A wiped hard drive shall be tested to ensure the information cannot be retrieved.
 - 3.1.3. Backup tapes, memory sticks, USB flash drives, CD ROMS and floppy disks shall be physically destroyed before disposing of them.
4. **Media Re-use**
 - 4.1. All **PHI** will be removed from the hard drives when the equipment is transferred to a workforce member who does not require access to the **PHI** or when the equipment is transferred to a new workforce member with different **PHI** access needs.
 - 4.1.1. Hard drive shall be wiped clean before transfer.



HIPAA SECURITY POLICIES

COUNTY OF PLACER

4.1.2. The hard drive shall be tested to ensure the information cannot be retrieved.

5. Computer Server Repair

5.1. When sending a computer server hard drive to repair:

5.1.1. All **PHI** will be removed from the server.

5.1.2. If the removal of **PHI** is not feasible for any reason, the third party servicing the equipment must sign the County's Business Associate Agreement in accordance with *HIPAA Policy 012, Business Associate Relationships*.

5.2. Before moving a server that contains **PHI**, a retrievable exact copy obtained through the backup process must be confirmed.

6. Devices and Media Acquisition

6.1. The County will include security requirements and/or security specifications in information system acquisition contracts based on an assessment of risk.

7. Responsibilities

7.1. Managers/Supervisors

7.1.1. Managers/supervisors shall ensure that only workforce members who require the need to remove **PHI** from their facilities are trained and granted permission to do so.

7.1.2. That an inventory and a record of movement of hardware and electronic media devices, and/or storage devices within the control of the manager or supervisor is maintained.

7.1.3. Ensure that **workforce members** set their computer to automatically lock when the computer is not in use. This will be done by **IT** on County computers.

7.1.4. Ensure that all **PHI** is not viewable by unauthorized persons at workstations in offices under their management.

7.1.5. Provide polarized screens or other computer security screen overlay devices that can shield **PHI** where applicable.

7.1.6. Ensure the placement of computers is out of visual range of persons other than the authorized user.

7.2. Workforce Member

7.2.1. The **workforce member** shall request and get permission from their manager to use portable electronic devices that contain **PHI**.

7.2.2. The **workforce members** will only use electronic media devices approved and distributed by **IT**.

7.2.3. **Workforce members** will limit the quantity of **PHI** on portable electronic devices to that which is necessary to perform their job duties.



HIPAA SECURITY POLICIES

COUNTY OF PLACER

- 7.2.4. **Workforce members** will report to their immediate supervisor any lost or stolen electronic media device containing **PHI**.
- 7.3. **IT**
- 7.3.1. For any electronic media with the control of IT, IT staff will ensure:
- 7.3.1.1. All hard drives are wiped clean before re-use or disposal.
 - 7.3.1.2. All hard drives are tested to ensure they have been cleaned.
 - 7.3.1.3. Backups of the **PHI** have been confirmed before hard drives are sent for repair.
 - 7.3.1.4. That an inventory and a record of movement of hardware and electronic media devices, workstation, servers, storage devices is maintained.

Reference(s):

- 45 CFR 164.310(d)(1)

Contact(s):

- HIPAA Security Officer (see main internal HHS web page for contact information)



HIPAA SECURITY POLICIES

COUNTY OF PLACER

Policy Title:	<i>Access Control and Authentication</i>		
Policy Number:	14	Version:	1.0
Approved By:	HIPAA Security Officer/ Placer County Board of Supervisors		
Effective Date:	October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or Hybrid Business Associate-like entity.		

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.

Definition:

See *HIPAA Security Policy 01, Assigned Responsibility and Definitions* for definitions applicable to all policies.

Policy:

1. General

1.1. Information systems used to access **PHI** shall uniquely identify and authenticate workforce members.

2. Authentication- Verification

2.1. 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 include:

2.1.1. Unique user ID and passwords.

2.1.2. Biometric identification system.

2.1.3. Telephone callback.

2.1.4. Token system that uses a physical device for user identification.

2.1.5. Two forms of authentication for wireless remote access.

2.1.6. Information systems used to access **PHI** shall identify and authenticate connections to specific devices involved in system communications.



HIPAA SECURITY POLICIES

COUNTY OF PLACER

3. Unique User ID and Password Management

- 3.1. All County **workforce members** that access **PHI** are to be assigned a unique user ID to access the network.
- 3.2. All **workforce members** are responsible for creating and maintaining the confidentiality of the password associated with their unique user ID.
- 3.3. Managers are required to ensure that their staff understands the user responsibilities for securely managing confidential passwords.
- 3.4. Upon receipt of a user ID, the member assigned the user ID is required to change the password provided by the administrator to a password that only he/she knows.
- 3.5. Effective passwords shall be created in order to secure access to **PHI**.
- 3.6. **Workforce members** who suspect that their password has become known by another person shall change their password immediately.
- 3.7. No user/**workforce member** shall give his or her password to another person.
- 3.8. **Workforce members** that access **PHI** are required to change their network password every 90 days.
- 3.9. Where technically feasible, **IT** will notify the **workforce member** via the network at least 7 days prior to the end of the 90 day period that they will need to select a new password.

4. Emergency Access to a User Account

- 4.1. In the event that access to a user account is required such as during a **workforce member's** absence for any reason, the following is required:
 - 4.1.1. A written request identifying the name of the user and the name of the contact to work with must be sent from the **HHS** Department Head or delegate to the **IT** Department Head or delegate for access to the user account.
 - 4.1.2. **IT** will change the user's password and securely deliver a temporary password to the contact person identified in the email request.
 - 4.1.3. The contact person named in the email must log in to the absent user's account and change the temporary password to one that only the contact person knows.
 - 4.1.4. Upon return of the absent user, the contact person must work with the returning user to have the returning user change the account password to something that only the returning user knows.
 - 4.1.5. All parties that obtain passwords must be authenticated before the password can be delivered by another party, such as by calling the receiving party at a known phone number.



HIPAA SECURITY POLICIES

COUNTY OF PLACER

5. Responsibilities

5.1. Managers/Supervisors

5.1.1. Managers and supervisors are responsible to reinforce secure password use in their offices with emphasis on "no password sharing".

5.1.2. If access to another worker's account is required, managers/supervisors shall follow the *Emergency Access to a User's Account* section of this policy (section 4).

5.2. Workforce Member

5.2.1. The **workforce member** shall formulate a strong password using the following guidelines:

5.2.1.1. Do not create passwords that can be found in a dictionary.

5.2.1.2. Create passwords of eight characters or more.

5.2.1.3. Use a mix of letters (upper and lower case), numbers, and special characters where allowed.

5.2.1.3.1. The password should contain one lower-case and one upper case character where allowed.

5.2.1.3.2. The password should contain one number where allowed.

5.2.1.3.3. The password should contain one special character where allowed.

5.2.1.4. The password should be easy to remember and hard to guess.

5.2.1.5. Where allowed, consider using a "pass phrase" such as "I love Ch0colate!" replacing one or more letters with a special character or number such as "3" for "e" or "0" for "O."

5.2.2. The **workforce member** working with **PHI** must **never**:

5.2.2.1. Reveal a password over the phone to any un-authenticated party.

5.2.2.2. Reveal a password in an e-mail message.

5.2.2.3. Reveal a password to their immediate supervisor unless required for emergency access, in which case section 4 of this document, *Emergency Access to a User Account* must be adhered to.

5.2.2.4. Reveal a password to an unknown party.

5.2.2.5. Reveal a password to co-workers.

5.2.2.6. Reveal a password on questionnaires or security forms.

5.2.2.7. Discuss a password in front of others.

5.2.2.8. Hint at the format of a password.

5.2.2.9. Share a County password with family members.



HIPAA SECURITY POLICIES

COUNTY OF PLACER

- 5.2.2.10. Use words such as “password”, “secure”, “secret”, “confidential”, “restricted”, or “private” as your password.
 - 5.2.2.11. Record a password and place it where others may obtain it.
 - 5.2.2.12. Misrepresent themselves by using another person’s user ID and password.
 - 5.2.2.13. Re-use passwords in whole or in part within the last ten required password intervals.
 - 5.2.2.14. Use any County password for any other system outside of the County.
 - 5.2.2.15. Use any part of the user’s name in the password.
 - 5.2.3. The **workforce member** may request a password change from **IT** at any time in cases where she/he cannot do so themselves.
 - 5.2.4. The **workforce member** must change their password if they suspect their password has been compromised.
- 5.3. **IT**
- 5.3.1. **IT** will provide the password for a new unique user ID to only the user to whom the new ID is assigned.
 - 5.3.2. **IT** 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 before fulfilling the request.

Reference(s):

- 45 CFR 164.312(a)(1)

Contact(s):

- HIPAA Security Officer (see main internal HHS web page for contact information)



HIPAA SECURITY POLICIES

COUNTY OF PLACER

Policy Title:	<i>Transmission Security, Integrity Controls and Encryption</i>		
Policy Number:	15	Version:	1.0
Approved By:	HIPAA Security Officer/ Placer County Board of Supervisors		
Effective Date:	October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or Hybrid Business Associate-like entity.		

Purpose:

The purpose of this policy is to guard against unauthorized access to, or modification of **PHI** that is being transmitted over an electronic communication network. When **PHI** is electronically transmitted from one point to another, it shall be protected by **encryption**.

Definition:

See *HIPAA Security Policy 01, Assigned Responsibility and Definitions* for definitions applicable to all policies.

Policy:

1. Transmission Encryption

- 1.1. Proven, standard algorithms shall be used as the basis for **encryption** technologies.
- 1.2. The use of proprietary **encryption** algorithms is not allowed for any purpose unless authorized by the HIPAA Security Officer.
- 1.3. No **PHI** shall be sent outside the secured County internal network over the Internet unless it is encrypted, including but not limited to:
 - 1.3.1. All email and email attachments containing **PHI** sent over the public Internet.
 - 1.3.2. Remote work sessions when a **workforce member** remotely connects to either the County Enterprise Network or a cloud-based application over the Internet to process **PHI**.
 - 1.3.3. Encryption of **PHI** is not required when the communication link is dedicated and not publicly shared from point-to-point, such as over a private "T1" connection or direct dial up modem.

2. Prohibited Transmission Modes



HIPAA SECURITY POLICIES

COUNTY OF PLACER

- 2.1. Modems shall never be left connected to personal computers in "auto-answer" mode.
- 2.2. Connecting with a modem 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.
- 2.3. Using a modem to dial-in to a County Network Connected workstation is prohibited.
3. **Wireless transmission of PHI within the County**
 - 3.1. The transmission of **PHI** over a wireless network within Placer County domain is permitted if both of the following conditions are met:
 - 3.1.1. The local wireless network is using an authentication mechanism to ensure that wireless devices connecting to the network are authorized.
 - 3.1.2. The local wireless network is utilizing an encryption mechanism for all transmissions over the aforementioned wireless network and uses two types of authentication.
 - 3.2. If transmitting **PHI** over a wireless network that is not using an authentication and encryption mechanism, the **PHI** shall be encrypted before transmission.
4. **Perimeter Security**
 - 4.1. Any external connection to the Placer County Area network shall come through the perimeter security's point of entry.
 - 4.2. If determined safe by authorized **IT** staff, outbound services shall be initiated for internal address to external addresses.
 - 4.3. Inbound services shall be negotiated on a case by case basis with authorized **IT** staff.
 - 4.4. All **workforce members** connecting to the County Enterprise Network for use to process **PHI** shall sign the *Placer County Acknowledgement of Information Security Responsibility* that they have received, reviewed, and understand the County's HIPAA Security Policy.
5. **Firewall Controls to transmit PHI into and out of Placer County**
 - 5.1. Networks containing systems and applications with **PHI** shall implement perimeter security and access control with a firewall.
 - 5.2. Firewalls shall be configured to support the following minimum requirements:
 - 5.2.1. Limit network access to only authorized workforce members and entities.
 - 5.2.2. Limit network access to only legitimate or established connections.
 - 5.2.3. Console and other management ports shall be appropriately secured or disabled.



HIPAA SECURITY POLICIES COUNTY OF PLACER

- 5.3. The configuration of firewalls used to protect networks containing **PHI**-based systems and applications shall be submitted to the HIPAA Security Officer for review and approval.

Reference(s):

- 45 CFR 164.312(e)(1)

Contact(s):

- HIPAA Security Officer (see main internal HHS web page for contact information)



HIPAA SECURITY POLICIES

COUNTY OF PLACER

Policy Title:	<i>Information Security Evaluation</i>		
Policy Number:	16	Version:	1.0
Approved By:	HIPAA Security Officer/ Placer County Board of Supervisors		
Effective Date:	October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or Hybrid Business Associate-like entity.		

Purpose:

The Information Security Evaluation Policy details the periodic technical and non-technical evaluations of security safeguards that **HHS** performs in order to demonstrate and document the extent of its compliance with security policies, the HIPAA Security Regulations, and all other applicable and appropriate local, state, and federal Regulations that pertain to Information Security Controls.

This policy supports HIPAA Security Regulations, Administrative Safeguards Standard, 45 CFR 164.308(a)(8)(i), which requires that Placer County: *“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.”*

Definition:

See *HIPAA Security Policy 01, Assigned Responsibility and Definitions* for definitions applicable to all policies.

Policy:

1. General

- 1.1. Placer County will conduct periodic technical and non-technical evaluations of security safeguards, including policies, controls and processes in order to demonstrate and document the extent of its compliance with its security policies, and the HIPAA Security Regulations.



HIPAA SECURITY POLICIES COUNTY OF PLACER

- 1.2. Evaluations may be conducted in whole or part at various timed intervals as a random sampling of systems and controls tailored to the environmental or operational change.
- 1.3. The technical and non-technical assessments may be conducted more frequently as a result of environmental or operational changes in the Placer County environment. Changes that might trigger a re-evaluation include:
 - 1.3.1. An identified security incident or breach of confidential information.
 - 1.3.2. Evolving significant threats and risks to data security.
 - 1.3.3. Significant changes to Placer County's organizational or technical infrastructure.
 - 1.3.4. Significant changes to information security roles or responsibilities.
 - 1.3.5. Newly emerging security technologies and industry recommendations.
 - 1.3.6. New laws or regulatory requirements.
- 1.4. Evaluations will be conducted internally or by a third party.
- 1.5. Evaluations may be conducted in whole or by subsystem at various timed intervals or as a random sampling of systems and controls tailored to the environmental or operational change that initiated the need for the evaluation and will include:
 - 1.5.1. A review of Placer County's security policies and procedures to evaluate their appropriateness and effectiveness at protecting against any reasonably anticipated threats or hazards to the confidentiality, integrity and availability of **PHI** and a gap analysis to compare the policies and procedures against actual practices.
 - 1.5.2. An identification of threats and risks to Placer County's systems and data.
 - 1.5.3. An assessment of Placer County's security controls and processes as reasonable and appropriate protections against the risks identified for the systems and confidential data.
 - 1.5.4. Testing and verification of Placer County's security controls and processes to determine whether they have been implemented properly and whether those controls and processes appropriately protect Placer County's **PHI**. This testing may be conducted by an authorized **workforce member** or a third party acting on Placer County's behalf.
- 1.6. The evaluation process and results are documented in a report that is provided to the HIPAA Security Officer.
- 1.7. Following each evaluation, Placer County will update its security policies, procedures, controls and processes as needed and where technically feasible to protect against any reasonably anticipated threats or hazards to the



HIPAA SECURITY POLICIES

COUNTY OF PLACER

confidentiality, integrity and availability of Placer County's systems and data and to align with local, state, and federal regulations pertaining to security controls.

- 1.8. Documentation of the evaluation process and the report shall be completed and maintained by Placer County.

Reference(s):

- 45 CFR 164.308(a)(8)(i)

Contact(s):

- HIPAA Security Officer (see main internal HHS web page for contact information)



HIPAA PRIVACY POLICIES

COUNTY OF PLACER

Policy Title:	Definitions; Uses and Disclosures of Protected Health Information; Authorizations		
Policy Number:	001	Version:	2.0
Approved By:	Placer County HIPAA Privacy Officer/ Board of Supervisors		
Effective Date:	September 1, 2004. Revised October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or a Placer County HIPAA Hybrid Business Associate-like Entity.		

Purpose:

To specify how and under what circumstances client *Protected Health Information* can be used or disclosed.

Definitions Applicable to All HIPAA Privacy Policies:

Business Associate – With respect to Placer County, a person who on behalf of the County, but other than in the capacity of a County employee, performs or assists in the performance of a function or activity involving the use or disclosure of PHI, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing benefit management, practice management, and re-pricing; or any other function or activity regulated by Federal privacy regulations; or provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for Placer County, where the service involves disclosure of PHI from the County, or from another Business Associate of the County.

Business Associate-like Entity -- A Placer County department, division, office, program or employee of the County of Placer which meets the definitions of a business associate under HIPAA (see definition above) and which has been formally designated as being a Placer County HIPAA hybrid Business Associate-like entity.

Covered Entity or Hybrid Covered Entity -- A Placer County department, division, office, program or employee of the County of Placer which meets the definitions of a covered entity under HIPAA and has been formally designated as being a covered entity under the Placer County HIPAA hybrid covered entity designation.

De-identified Information -- Is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual.

HIPAA – (The Health Insurance Portability and Accountability Act of 1996) A federal law that protects health insurance coverage for individuals and requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.

Limited Data Set -- Is PHI that excludes the following identifiers of the individual or of relatives, employers, or household members of the individual: Names; Postal address information, other than town or city, State, and zip code; Telephone numbers; Fax numbers; Electronic mail addresses; Social Security numbers; Medical record numbers; Health plan beneficiary numbers; Account numbers; Certificate/license numbers; Vehicle identifiers and serial numbers, including license plate numbers; Device identifiers and serial numbers; Web Universal Resource Locators (URLs); Internet Protocol (IP) address numbers; Biometric identifiers, including finger and voice prints; and Full face photographic images and any comparable images.

Protected Health Information (PHI) – Information that is under the control of a “covered entity” or its “Business Associates” that relates to the past, present, or future condition, either physical or mental, of an individual, identifying the individual or having enough information in it so that a reasonably prudent person would be able to identify the individual.

Workforce Members -- Placer County HIPAA Hybrid Covered Entity employees, volunteers, or interns, and/or Hybrid Business Associate-like entity employees, volunteers, or interns, who have access to PHI. **Placer County, County, County Employees, County Staff** -- All references in this Policy refer only to, as appropriate, Workforce Members.

Policy:

1. **Placer County may use or disclose a client’s *Protected Health Information* without an Authorization for:**

 - 1.1. Treatment,
 - 1.2. Payment, or
 - 1.3. Healthcare Operations

Note: Disclosure of *Protected Health Information* within the Department of Health & Human Services for the above purposes is permitted by this policy.

2. **Other ways the County may use or disclose information without an *Authorization* include the following legally recognized exceptions:**

2.1. **Public health activities**

We may provide *Protected Health Information* to public health or legal authorities charged with preventing or controlling disease, injury, or disability, including reporting of vital statistics.

2.2. **Victims of child or adult abuse, neglect, or domestic violence**

If we believe disclosure of information is necessary to prevent or discontinue serious harm to someone, that information may be shared with certain governmental agencies under certain circumstances. However, in the case of adult abuse, the alleged victim must be unwilling, unable or incapable of consenting.

2.3. **Health oversight activities**

We may provide health care information to certain agencies that oversee health care systems as part of their audits, civil, administrative or criminal investigations, inspections, and for licensures or disciplinary actions.

2.4. **Judicially-approved legal/administrative proceedings**

We may share health information for judicial and administrative purposes such as in lawsuits, subpoenas, warrants, or court orders. There are exceptions that should be reviewed with the Privacy Officer and/or County Counsel as appropriate.

2.5. **Law enforcement**

We may share health information for certain law enforcement purposes, including laws that require reporting of certain types of wounds or other physical injury or abuse, or on program premises. Sharing is also allowed to identify a suspect, fugitive, witness or missing person, with the exception of mental/behavioral health treatment information.

2.6. **Coroners, medical examiners, and funeral directors**

We may be required to share health information with these officials, in order for them to carry out their duties, e.g. identify next of kin.

2.7. **Organ procurement organizations**

We may share health information with organizations that obtain, store or transplant organs or tissue.

2.8. **Research**

We may share *Protected Health Information* with specific approved researchers who are also required to protect health information.

2.9. Immunization records

We may disclose information relating to a client's proof of immunization if required by State or other law for school admission with documentation of oral authorization.

2.10. Threat to health & safety

We may share health information in the case of a threat to the health or safety of a person or the public, such as a terrorist attack, medical emergencies, serious risk of disease, injury or disability, or emergency disaster relief.

2.11. For specialized governmental functions

We may share health information for reasons of national security, intelligence or to public assistance programs.

2.12. Correctional institutions

We may legally share *Protected Health Information* with the healthcare staff of a correctional institution such as the Placer County Jail, or law enforcement official having custody of an inmate for the purpose of providing health care or ensuring the health and safety of individuals or other inmates.

2.13. In case of an emergency, to the extent needed to provide emergency treatment.

2.14. We may provide **clients or representatives** acting on their behalf with access to their own *Protected Health Information*, at their request.

2.15. To an individual assisting the client with care or payment for care, if the client has an opportunity to verbally consent or object, and to a deceased client's family provided Placer County did not receive an objection to such disclosure prior to the client's death.

2.16. To family members or close friends, if the client has an opportunity to verbally consent or object.

2.17. Business Associates

We may disclose *Protected Health Information* to a Business Associate, vendor or subcontractor in accordance with an applicable **Business Associate Agreement**.

2.18. Placer County HIPAA Hybrid Business Associate-like Entities.

We may disclose *Protected Health Information* to employees in those departments, divisions, offices and programs of the County of Placer which have been formally designated as Placer County HIPAA Hybrid Business Associate-like entities.

Placer County must also agree to a client's restrictions on the disclosure of a client's Protected Health Information to a client's health plan if the disclosure is for the purpose of carrying out payment, is not otherwise required by law, and the client has paid Placer County in full for services rendered.

SPECIFIC AUTHORIZATIONS AND RESTRICTIONS ON USES AND

DISCLOSURES OF PHI: Unless a legal exception is identified by the Privacy Officer or County Counsel, specific authorizations are required for the use and/or disclosure of the following:

- a) Psychotherapy notes;
 - b) HIV-related information;
 - c) Alcohol and/or substance abuse records;
 - d) Sexually transmitted diseases;
 - e) Mental health records;
 - f) Genetic information;
 - g) Research (unless specifically approved by authorized Placer County management);
 - h) Marketing involving direct or indirect remuneration to Placer County for the PHI;
 - i) Fundraising activities, unless the use or disclosure is only the client's name, address, other contact information, age, gender, date of birth, dates of health care provided, department of service information, treating physician, outcome information, and/or health insurance status; and,
 - j) Sale of PHI involving direct or indirect remuneration to Placer County for the PHI. This does not include the exchange of PHI:
 - 1. For public health purposes;
 - 2. For research purposes, if Placer County receives only a cost-based fee to prepare and transmit the client information;
 - 3. For treatment or payment for treatment;
 - 4. For the sale, transfer, merger or consolidation of Placer County; and,
 - 5. To a Business Associate, if Placer County only receives remuneration for the performance of health care related activities.
3. **Placer County must obtain a completed and signed *Authorization for Release of Information* for:**
- 3.1. Enrollment in a County administered health plan, if necessary for determining eligibility;
 - 3.2. Disclosures to a client's employer for employment purposes;
 - 3.3. Research purposes unrelated to the client's treatment; and
 - 3.4. Any purpose in which State or Federal law requires a signed *Authorization*.
4. **Placer County will only honor a valid, *HIPAA-compliant Authorization* that is signed and dated by the client or the client's legal representative. The County's *Authorization* will be regarded as a separate document; the County will not print other information on the *Authorization* in an effort to consolidate or combine documents.**
5. **When a client or parent wishes to authorize multiple providers to receive the same *Protected Health Information*, the responsible County Division may add a sheet that lists the providers. The client or parent must initial each name on the list, to serve as verification that each provider may have access to the same *Protected Health Information*.**

6. **In the case of a family with multiple children**, a separate and distinct *Authorization* must be completed for each child, as each child's *Protected Health Information* is unique and singularly protected.

7. Authorization Required Components:

Although it need not be a Placer County form, the *Authorization* must include the following core elements, in 14-point font:

- Name of client whose records are requested
- Name of party (or entity) in possession of records
- Name, address and telephone number of recipient of information
- Detailed description of information requested (if not entire record)
- Reason for request (purpose)
- Date (or event) that will cause *Authorization* to expire
- If request is for or includes information regarding mental health, substance abuse, HIV/AIDS, sexually transmitted diseases, or genetic testing, such information must be specifically named in order to be included in the information released.
- Individual's right to revoke the *Authorization* in writing
- Exceptions to the right to revoke
- Description of how to revoke
- Reference to *Notice of Privacy Practices*, if applicable
- Ability or inability to condition open enrollment or eligibility (not always applicable)
- Consequences of not signing if treatment, enrollment or eligibility conditioned upon (not always applicable)
- Potential for re-disclosure
- Signature and date
- Client's right to a copy (if information sought by covered entity)

8. Revocation of *Authorization*

- 8.1. An individual can revoke a previously signed *Authorization* at any time except for information that has already been released.
- 8.2. A revocation must be in writing and signed and dated by the client.
- 8.3. *Authorizations* to disclose substance abuse records may be revoked orally and must be documented in the client's record.

9. Verification of Individuals Requesting Information

Information about a client may not be disclosed without verifying the identity of the person requesting the information, if the authorized staff member fulfilling the request does not know that person.

10. Who may Authorize Disclosures:

The following individuals may sign an *Authorization for Release of Information*:

- 10.1. The client about whom the information is generated if he/she is a competent adult;
- 10.2. A minor, if legally able to consent to treatment without parental consent under State law;
- 10.3. Any minor, if treatment is for rape or sexual assault;
- 10.4. Other minors, if:
 - 10.4.1. Minor is emancipated, or
 - 10.4.2. Treatment is related to the prevention of or treatment for pregnancy, or
 - 10.4.3. Minor is 12 years old or older and treatment is related to communicable disease, sexually transmitted diseases, alcohol or drug abuse, or mental health.
- 10.5. A parent or legal guardian of minor if he/she is not legally able to consent to treatment; or
- 10.6. The client's legal representative if the client is deceased or lacks the ability to authorize the disclosure on his or her own behalf.

Form:

- “*Authorization for Release of Information*”

Reference(s):

- 45 CFR 164.502(a)
- 45 CFR 164.506 – 164.512
- 42 CFR Part 2
- Cal. Civil Code § 56.10 et seq.
- Cal. Health & Safety Code § 121025 et seq.
- Cal. Welfare & Institutions Code § 5328 et seq.

Contact:

- Placer County HIPAA Privacy Officer. See main internal HHS web page, HIPAA contact page on County website, and current Placer County Telephone Directory for contact information.



HIPAA PRIVACY POLICIES

COUNTY OF PLACER

Policy Title:	Clients' Right to Access Their <i>Protected Health Information</i>		
Policy Number:	002	Version:	3.0
Approved By:	Placer County HIPAA Privacy Officer/Board of Supervisors		
Effective Date:	September 1, 2004. Revised October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or a Placer County HIPAA Hybrid Business Associate-like Entity.		

Purpose:

To describe the right that Placer County clients have regarding the access to their own *Protected Health Information* held by the County, and to describe the circumstances under which access may be denied.

Definition:

For Definitions applicable to this and all HIPAA Privacy Policies, see the Definitions section of HIPAA Privacy Policy 001, "Definitions; Uses and Disclosures of Protected Health Information; Authorizations".

Who Can Access: A client, a client's guardian, or a client's personal representative may access a record after submitting a written request to physically inspect or receive a copy of the medical record. A client or client's personal representative is any client, parent, guardian, or committee of an incompetent.

What Information: Placer County's clients have the right to inspect and obtain a copy of the protected health information that Placer County, or one of its Business Associates, maintains in "designated record sets." "Designated record sets" are sets of records that may be used to make decisions about the clients or their treatment.

The designated record set for each client generally includes the client's medical record.

For How Long: A client, a client's legal guardian, or a client's personal representative may access a record. Clients must submit a written request to physically inspect or receive a copy of the medical record. Clients have the right to access their protected health information for as long as the information is contained in their designated record set.

Proper Identification: In the interest of protecting the confidentiality of the record, the person requesting access should present identification such as a government issued picture card, a driver's license or ID card that carries a valid signature. Individuals requesting

access in the capacity of guardian or conservator of the person should send a copy of their appointment papers when requesting copies or present such papers at the time of inspection. The signature will be compared with the signature on the consent for treatment and any discrepancy clarified.

Policy:

1. Right of clients to access and/or obtain a copy of his/her information

- 1.1. Clients have the right to access, inspect, and obtain a paper or electronic copy of ***Protected Health Information*** on their own cases in County files or records, consistent with Federal and State law. Placer County must provide the client a copy in the electronic form and format requested, as long as Placer County can readily produce such information in the form requested. Otherwise, Placer County should cooperate with the client to provide a readable electronic form and format of the records as agreed between Placer County and the client.
- 1.2. All requests for access will be made in writing by having the client complete an ***“Access to Records Request Form.”*** Each County Division will have a Policy that describes where in the client’s record the signed “Access to Records Request Form” will be placed.
- 1.3. **The County must:**
 - 1.3.1. Provide access (inspection) within five (5) working days of receipt or the ***Request***, and
 - 1.3.2. Provide a copy within fifteen (15) calendar days of receipt of the ***Request***.
- 1.4. If Placer County maintains information about the client in a record that includes ***Protected Health Information*** about other people, the client is only authorized to see information about himself or herself, except as provided below:
 - 1.4.1. If a person identified in the file is a minor child of the client, and the client is authorized under California law to have access to the minor’s information or to act on behalf of the minor for making decisions about the minor’s care, the client may also obtain information about the minor.
 - 1.4.2. If the person requesting information is recognized under California law as a guardian or legal custodian of the client and is authorized by California law to have access to the client’s information or to act on behalf of the client for making decisions about the client’s services or care, the County will release information to the requestor.

If a client’s personal representative requests access to the client’s records, the Privacy Officer generally should grant or deny access according to the procedures in this policy as though the client personal representative were the client, unless one of the following exceptions applies:

Client Lacking Capacity: When a client lacks capacity to make health care decisions and the client’s personal representative must be given access to the client’s information in order to make health care decisions on behalf of the client, the Privacy Officer should

grant such access to the client's personal representative.

Clients Who have Expired: A deceased patient's beneficiary or personal representative will have the same right of access as the patient would have had if he or she were still living. The beneficiary is anyone who will inherit from the patient by will or estate. The personal representative is either the administrator of the patient's estate or the executor under the patient's will. The law does not give any other person the right to obtain access to a deceased patient's records. Legal documentation must be provided to prove one is the "personal representative" of a deceased patient.

Documentation: The Privacy Officer must keep the documentation in connection with any request by a client or a client's personal representative to access protected health information. These documents must be maintained by Placer County for seven (7) years from the date of their creation. When possible, these documents will be kept in the client's medical record.

2. Denial of Access

2.1. Placer County may deny clients' access to their own *Protected Health Information* if Federal law prohibits the disclosure.

2.1.1. Before Placer County denies a client access to his or her own *Protected Health Information*, the County decision to deny must be made by a licensed health care professional or other designated staff, and the County must make a review of this denial available to the client. If the client wishes to have this denial reviewed, the review must be done by a licensed health care professional who was not involved in the original decision.

2.2. Placer County may deny the request if it is not in writing.

2.3. The following requests that are denied are **NOT REVIEWABLE**:

2.3.1. Information compiled in anticipation of use in civil, criminal, or administrative proceedings;

2.3.2. Information that is subject to the Federal *Clinical Labs Improvement Amendments of 1988 (CLIA)*, or exempt pursuant to 42 CFR 493.3(a)(2);

2.3.3. Documents protected by attorney work-product privilege;

2.3.4. Information on other persons the client is not authorized to access;

2.3.5. Information where release is prohibited by State or Federal laws;

2.3.6. Information obtained confidentially from non-provider and access would reveal that source;

2.3.7. Access suspended temporarily due to ongoing research program;

2.3.8. If the County is acting under the direction of a correctional institution and access could endanger the health, safety, security, custody or rehabilitation of the inmate or someone else.

2.4. The following requests that are denied are **REVIEWABLE**:

2.4.1. Information that a licensed health care professional has determined, in the exercise of professional judgment, is reasonably likely to:

- (a) Endanger the life or physical safety of the individual or another person,
OR
- (b) Makes reference to another person to whom substantial harm could be caused, **OR**
- (c) The request for access is made by the individual's personal representative and such access could cause substantial harm to the individual or another person.

Form:

- *“Access to Health Records Request”*

Reference(s):

- *45 CFR Part 164.522 – 164.528*
- *Cal. Health & Safety Code § §123100 et seq.*

Contact:

- Placer County HIPAA Privacy Officer. See main internal HHS web page, HIPAA contact page on County website, and current Placer County Telephone Directory for Contact information.



HIPAA PRIVACY POLICIES

COUNTY OF PLACER

Policy Title:	<i>Minimum Necessary</i> Information		
Policy Number:	003	Version:	2.0
Approved By:	Placer County HIPAA Privacy Officer/Board of Supervisors		
Effective Date:	September 1, 2004. Revised October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or a Placer County HIPAA Hybrid Business Associate-like Entity.		

Purpose:

To improve the privacy of confidential information that is used or disclosed by Placer County employees in the course of their work; and

To ensure that Placer County employees have access to the information they routinely require to accomplish their mission, goals and objectives.

Definition:

For Definitions applicable to this and all HIPAA Privacy Policies, see the Definitions section of HIPAA Privacy Policy 001, "Definitions; Uses and Disclosures of Protected Health Information; Authorizations".

Policy:

1. General

1.1. Placer County will use or disclose only the *minimum amount of information necessary* to provide services and benefits to clients, and only to the extent provided in County policies and procedures. Placer County will not disclose an entire medical record unless specifically requested by the client or specific justification is documented.

1.2. This policy does not apply to uses or disclosures:

1.2.1. To or from a health care provider for treatment of the individual client;

1.2.2. To the individual about his or her own *Protected Health Information*;

1.2.3. Authorized by the individual that are within the scope of a valid *Authorization for Release of Information*;

1.2.4. Required by law;

- 1.2.5. Required for compliance with the *HIPAA Transaction Rule*;
- 1.2.6. To the U.S. Department of Health & Human Services; and
- 1.2.7. Outlined in the Placer County Policy, "***Uses and Disclosures of Protected Health Information***"

2. **Minimum Necessary Information**

- 2.1. For all permitted disclosures of ***Protected Health Information***, we must make reasonable efforts to limit the amount of information to the ***minimum necessary*** needed to accomplish the intended purpose of the use, disclosure, or request.
- 2.2. Although Placer County relies on representations that ***Protected Health Information*** received is the "***minimum necessary***" as described above, we will inquire or seek clarifications or modifications when deemed appropriate.
- 2.3. When determining the degree of information to disclose to meet the "***minimum necessary***" test, we can and should honor requests from:
 - 2.3.1. Authorized public officials;
 - 2.3.2. All covered entities (health plans, health care providers, and health clearinghouses) and authorized members of their workforces if the disclosure is for treatment, payment, and/or healthcare operations;
 - 2.3.3. A person requesting the information for research purposes that has complied with the applicable requirements of Placer County Policy, "***Uses and Disclosures for Research Purposes & Waivers***".
- 2.4. All questions relating to non-routine requests will be referred to the Privacy Officer or the Office of County Counsel.
- 2.5. Entire Medical File: Placer County will not disclose an individual's entire medical record unless the request specifically justifies why the entire medical record is needed and applicable law permits such a disclosure or the client requests such a disclosure.

3. **Access & Uses of Information:**

- 3.1. Placer County will establish role-based categories that identify types of information necessary for employees to do their jobs. Placer County's program areas will identify the category of information needed for persons, or classes of persons, in their respective workforces to carry out their duties, and will further identify any conditions appropriate to such access. Categories will include all information, such as information accessible by computer, kept in files, or other forms of information consistent with Placer County Policy, "***Administrative, Technical and Physical Safeguards.***"

Reference(s):

- 45 CFR Parts 160 and 164

Contact(s):

- Placer County HIPAA Privacy Officer. See main internal HHS web page, HIPAA contact page on County website, and current Placer County Telephone Directory for contact information.



HIPAA PRIVACY POLICIES

COUNTY OF PLACER

Policy Title:	Providing Clients with <i>Notice of Privacy Practices</i> and Obtaining <i>Acknowledgement of Receipt</i>		
Policy Number:	004	Version:	2.0
Approved By:	Placer County HIPAA Privacy Officer/Board of Supervisors		
Effective Date:	September 1, 2004. Revised October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or a Placer County HIPAA Hybrid Business Associate-like Entity.		

Purpose:

To describe the circumstances under which a *Notice of Privacy Practices* will be provided to Placer County clients. Anyone may be provided with a copy of the *Notice* – distribution is not limited to current clients, patients, or enrollees. The *Notice* is intended to be a public document that people may use to inform themselves as to our current efforts and exceptions regarding the safeguarding and maintenance of confidential patient information.

Definition:

For Definitions applicable to this and all HIPAA Privacy Policies, see the Definitions section of HIPAA Privacy Policy 001, "Definitions; Uses and Disclosures of Protected Health Information; Authorizations".

Policy:

1. As a HEALTH PROVIDER, Placer County will:

- 1.1. Provide the *Notice* no later than the first date of the first service delivery. If the first service is delivered electronically, the *Notice* will be sent electronically, automatically and contemporaneously. The *Notice* will be provided at the point of registration for health care services.
- 1.2. Make the *Notice* available for individuals to take with them.
- 1.3. Post the *Notice* in a clear and prominent location where it is reasonable to expect individuals to be able to read.

1.4. Post the *Notice* prominently on any web site containing information about Placer County's health care services and make the *Notice* available electronically through the County's internet web site.

1.5. Within 60 days of a material revision of the *Notice*, it will be posted and made available to clients upon request.

2. **As a HEALTH PLAN, Placer County will:**

Provide *Notice* no later than April 14, 2003, to individuals then covered by any County health plan. The primary applicant will receive the *Notice*, not the dependents.

2.1. Provide the *Notice* to all new individuals at the time of enrollment in the health plan.

2.2. Notify all individuals then covered by the plan every three years of the availability of the *Notice* and how to obtain the *Notice*.

2.3. No less frequently than once every three years, notify the individuals then covered by the Plan of the availability of the *Notice* and how to obtain a copy.

3. **General provisions applicable to the County as a health care provider and as a health plan:**

3.1. Who Will Be Provided With a *NOTICE*:

3.1.1. The client about whom the information is generated if:

3.1.1.1. He/she is a competent adult; or

3.1.1.2. A minor authorized under applicable State law to independently consent to treatment, including the following types of minors:

- Self-sufficient (15 years or older, not living at home, manages own financial affairs),
- Treatment related to prevention of or treatment for pregnancy, or
- Treatment or prevention of communicable disease, sexually transmitted diseases, rape and sexual assault (minors of any age), alcohol or drug abuse, or mental health services (minors 12 years or older).

3.1.2. A parent or legal guardian on behalf of a minor child if he/she is not authorized under State law to control the use or disclosure of his/ her *PHI*; or

3.1.3. The individual's legal representative if the individual is deceased or lacks the ability to authorize the disclosure on his or her own behalf.

3.2. Special Circumstances

3.2.1. If the individual receiving services is **PERMANENTLY incapacitated or is being seen on an emergency basis**, the *Notice* may be provided to a legal representative, or if none exists or is known, then to the next of kin, having that individual sign the *Acknowledgement of Receipt*.

- 3.2.2. If the individual receiving services is **TEMPORARILY incapacitated or is being seen on an emergency basis**, the *Notice* and *Acknowledgement* will be held with any other documents requiring the individual's signature until the individual regains capacity or within a reasonable period of time after the emergency situation.
- 3.2.3. **If a minor can consent to treatment on his/her own behalf**, the *Notice* is provided to him/her for their signature. Otherwise, it is provided to the parent, legal guardian or personal representative.
- 3.2.4. **Pharmacy patients:** If the County pharmacy provides medication prescriptions to individuals who have not been registered in the County healthcare system, the *Notice* will be provided to the person who picks up the prescription.
- 3.2.5. **Inmates in County correctional facilities** will NOT be provided a *Notice* while they are incarcerated.
- 3.2.6. **For clients with disabilities:** Staff will provide alternative forms of notice at the earliest possible opportunity, when the need arises, such as reading the *Notice* aloud to individuals upon request.
- 3.3. Assigned Placer County staff will make a good faith effort to obtain the signed *Acknowledgment of Receipt*. If the individual refuses to sign, staff will document the effort made and why the form was not signed.

Alternative means of acknowledging receipt are acceptable, such as:
 - 3.3.1. The client signing a separate paper or log book.
 - 3.3.2. The client initialing a page of the *Notice* that the County retains.
 - 3.3.3. The client providing an electronic *Acknowledgement*.
- 3.4. The *Notice* will be regarded as a separate document; the County will not print other information on the *Notice* in an effort to consolidate or combine documents.
- 3.5. Retention of Documentation

Signed and unsigned *Acknowledgments* will be filed with the individual's medical record and will be retained in accordance with County policies for record retention.
- 3.6. Revisions to the *Notice of Privacy Practices*

The County will promptly revise and distribute its *Notice* whenever there is a material change to the uses or disclosures, individual's rights, the County's legal duties, or other privacy practices stated in the *Notice*. The County will distribute the *Notice* within sixty (60) days to all individuals then covered by the applicable plan. Except when required by law, a material change to any term of the *Notice* may not be implemented prior to the effective date of the *Notice* in which the material change is reflected.

Form(s):

- *“Notice of Privacy Practices”*
- *“Acknowledgement of Receipt”*

Reference(s):

- *45 CFR Part 164.520 – 164.528*

Contact(s):

- Placer County HIPAA Privacy Officer. See main internal HHS web page, HIPAA contact page on County website, and current Placer County Telephone Directory for contact information.



HIPAA PRIVACY POLICIES

COUNTY OF PLACER

Policy Title:	Privacy Complaints		
Policy Number:	005	Version:	2.0
Approved By:	Placer County HIPAA Privacy Officer/Board of Supervisors		
Effective Date:	September 1, 2004. Revised October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or a Placer County HIPAA Hybrid Business Associate-like Entity.		

Purpose:

To describe the right that Placer County clients, employees, and Business Associates have to file complaints if they feel that a breach of privacy has occurred regarding **Protected Health Information** held by the County, and to describe the process for filing a complaint.

Definition:

For Definitions applicable to this and all HIPAA Privacy Policies, see the Definitions section of HIPAA Privacy Policy 001, "Definitions; Uses and Disclosures of Protected Health Information; Authorizations".

Policy:

1. Placer County clients, employees, and Business Associates have the right to submit complaints if:
 - 1.1. They believe or suspect that **Protected Health Information** has been improperly used or disclosed by the County, its workforce, or a Business Associate of the County;
 - 1.2. They have concerns about the privacy policies of Placer County or a Business Associate of the County;
 - 1.3. They have concerns regarding the denial of access to or amendments of their **Protected Health Information**;
 - 1.4. They believe or suspect that they have been retaliated against or intimidated by members of the County workforce because they have not authorized the release of their **Protected Health Information**.

2. Complainants must be advised that they may file complaints with the County or with the U.S. Department of Health and Human Services, Office for Civil Rights.
3. Placer County will not intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against any person filing a complaint or inquiring about how to file a complaint.
4. Placer County may not require clients to waive their rights to file a complaint as a condition of providing treatment, payment enrollment in a health plan, or eligibility for benefits.
5. The County must provide complainants with the specific person or office and address of where to submit written complaints:

Privacy Officer
Placer County Department of Health & Human Services
3091 County Center Drive, Suite 290
Auburn, California 95603
Telephone: (530) 886-3621

Or

U.S. Department of Health & Human Services
Office for Civil Rights
90 7th Street, Suite 4-100
San Francisco, CA 94103
Phone: (800) 368-1019
TDD: (800) 537-7697
FAX: (415) 437-8329

6. An individual filing a complaint has 180 days from the date he or she becomes aware of the suspected violation to file a complaint with the U.S. Department of Health & Human Services. Individuals who wish to file a privacy-related complaint with the County are encouraged to do so as soon as they become aware of a suspected violation, to facilitate investigation of the complaint and corrective action. Complaints will be kept confidential to the extent possible, but a complaint filed anonymously cannot be properly investigated.
7. The Privacy Officer will review and determine action on complaints filed with County and make an effort to immediately mitigate any harmful effects that may have occurred. The Privacy Officer will also perform these functions when the County is contacted about complaints filed with the U.S. Department of Health & Human Services, Office for Civil Rights.

8. To the extent allowed by State and Federal law, the Privacy Officer will inform the individual within 60 calendar days of filing the complaint about the results of the investigation, and what corrective actions have been taken if any are necessary, or why corrective actions are not needed.
9. The Privacy Officer will document all complaints, the findings from reviewing each complaint, and County actions resulting from the complaint. This documentation shall include a description of corrective actions that the County has taken, if any are necessary, or of why corrective actions are not needed, for each specific complaint. The documentation will be maintained for a minimum of six years following the disposition of the complaint.

Form(s):

- *“Health Information Privacy Complaint Form”*

Reference(s):

- *45 CFR Part 164.522 – 164.528*

Contact(s):

- Placer County HIPAA Privacy Officer. See main internal HHS web page, HIPAA contact page on County website, and current Placer County Telephone Directory for contact information.



HIPAA PRIVACY POLICIES COUNTY OF PLACER

Policy Title:	Client Requests for Restrictions on <i>Protected Health Information</i>		
Policy Number:	006	Version:	3.0
Approved By:	Placer County HIPAA Privacy Officer/Board of Supervisors		
Effective Date:	September 1, 2004. Revised October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or a Placer County HIPAA Hybrid Business Associate-like Entity.		

Purpose:

To describe the right that Placer County clients have regarding the restriction on the use and/or disclosure of their *Protected Health Information*.

Definition:

For Definitions applicable to this and all HIPAA Privacy Policies, see the Definitions section of HIPAA Privacy Policy 001, "Definitions; Uses and Disclosures of Protected Health Information; Authorizations".

Policy:

Placer County clients have a right to request restrictions on the use and/or disclosure of their own *Protected Health Information* while carrying out treatment, payment activities, or health care operations. Placer County clients also have the right to request that their health information not be disclosed to a health plan if they have paid for the services in full, and the disclosure is not otherwise required by law. The request for restriction will only be applicable to that particular service. The client will have to request a restriction for each service thereafter.

1. All requests will be made by completing a "*Restriction of Use and Disclosures Request Form*" and submitting it to the Privacy Officer. All restrictions agreed to by the County must accompany the client's medical or billing record, to ensure that the restrictions are understood and respected. Documentation of restriction requests and County decisions pertaining to them will be maintained for a minimum of six (6) years after taking effect.

- 1.1. Placer County is not obligated to agree to a restriction and may deny the request or may agree to a restriction more limited than what the client requested. In either

case, the client will be given the opportunity to discuss the concerns.

Placer County will not agree to restrict uses or disclosures of ***Protected Health Information*** if the requested restriction would adversely affect the quality of the client's care or services prevent or limit the County from making or obtaining payment for services.

2. **Exception to restrictions:**

If the client needs emergency treatment and the restricted information is needed to provide such treatment, Placer County may use or disclose such information to the extent needed to provide it. However, once the emergency situation subsides, the County must ask the provider not to re-disclose the information.

3. **Exception to denial of restrictions:**

For Substance Abuse or Vocational Rehabilitation participants, Federal regulations prohibit Placer County from denying client requests for restrictions on uses and disclosures of their ***Protected Health Information*** regarding treatment or rehabilitation.

3.1. Placer County may terminate a restriction if:

3.1.1. The client agrees to or requests termination of the restriction in writing (or orally, if documented in writing), or

3.1.2. The County informs the client in writing that the County is terminating its agreement to the restriction. Information created or received while the restriction was in effect shall remain subject to the restriction.

3.2. Restrictions are not applicable to uses and disclosures for which an ***Authorization*** is not required. These include:

3.2.1. Public Health activities

3.2.2. Reporting abuse, neglect or domestic violence

3.2.3. Health oversight agencies

3.2.4. Judicial or administrative proceedings

3.2.5. Disclosures for law enforcement purposes

3.2.6. Certain disclosures for decedents

3.2.7. Certain organ donation purposes

3.2.8. Certain research activities

3.2.9. Certain Workers' Compensation activities

3.2.10. National security and intelligence activities

3.2.11. Medical suitability determinations

3.2.12. Eligibility functions related to government programs providing public benefits

4. Prior to any use or disclosure of client information, County staff must confirm that such use or disclosure has not been granted a restriction by reviewing the client's case file.
5. If the County agrees to a client's request for restriction, the County will flag the designated record to inform subsequent personnel that a restriction exists. Others may be informed of the restriction without disclosing any of the restricted information. The restriction only binds the covered component of the County (and *Business Associates*) and does not bind other entities to which information may be further disclosed. The client will be notified in writing of the decision and of any perceived potential consequences of the decision.
6. The County will document the client's request, and the reasons for granting or denying the request in the client's hard copy or electronic County case record file. A denial of the restriction must be in writing to the client.

Form(s):

- *"Restriction of Use and Disclosures Request Form"*

Reference(s):

- 45 CFR Part 164.522 – 164.528
- 42 CFR Part 2
- 34 CFR

Contact(s):

- Placer County HIPAA Privacy Officer. See main internal HHS web page, HIPAA contact page on County website, and current Placer County Telephone Directory for contact information.



HIPAA PRIVACY POLICIES

COUNTY OF PLACER

Policy Title:	Alternative Means of Communicating with Clients		
Policy Number:	007	Version:	2.0
Approved By:	Placer County HIPAA Privacy Officer/Board of Supervisors		
Effective Date:	September 1, 2004. Revised October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or a Placer County HIPAA Hybrid Business Associate-like Entity.		

Purpose:

To describe the right that Placer County clients have regarding their receipt of communications by alternative means, and to describe the circumstances under which alternative means of communications may be denied or terminated.

Definition:

For Definitions applicable to this and all HIPAA Privacy Policies, see the Definitions section of HIPAA Privacy Policy 001, "Definitions; Uses and Disclosures of Protected Health Information; Authorizations".

Policy:

1. Placer County clients may receive *Protected Health Information* from the County by alternative means of communication.

Examples of the types of communication subject to this policy include requests to contact the client:

- At place of employment rather than residence;
- By mail;
- By fax;
- By telephone;
- By e-mail; or
- By sealed envelope rather than postcard.

2. Clients should always provide the County with at least one alternative means of communication.
3. Placer County must accommodate reasonable requests, as determined by the County, based solely upon the administrative difficulty in complying with the request.

4. Requests for alternative means of communication are preferable in writing. However, if made in person, by telephone, or electronically, the County will document the request and verify the client's identity.
5. Any request that is granted will be documented in the client's record in a clear and unambiguous manner that will alert staff that may be required to communicate with the client.
6. If a client's request cannot be met, Placer County will notify the client in writing.
7. Placer County will notify the client in writing if the arrangement is terminated, due to:
 - 7.1. Inability to contact the client at the location or in the manner requested;
 - 7.2. Ineffectiveness; or
 - 7.3. The client's failure to respond to communications.

Reference(s):

- 45 CFR Part 164.522 – 164.528

Contact(s):

- Placer County HIPAA Privacy Officer. See main internal HHS web page, HIPAA contact page on County website, and current Placer County Telephone Directory for contact information.



HIPAA PRIVACY POLICIES

COUNTY OF PLACER

Policy Title:	Amending Client Protected Health Information		
Policy Number:	008	Version:	2.0
Approved By:	Placer County HIPAA Privacy Officer/Board of Supervisors		
Effective Date:	September 1, 2004. Revised October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or a Placer County HIPAA Hybrid Business Associate-like Entity.		

Purpose:

To describe the right that Placer County clients have regarding the amending of their *Protected Health Information* that is held by the County.

Definition:

For Definitions applicable to this and all HIPAA Privacy Policies, see the Definitions section of HIPAA Privacy Policy 001, "Definitions; Uses and Disclosures of Protected Health Information; Authorizations".

Policy:

1. Placer County clients have the right to request that the County amend their *Protected Health Information* that is held by the County.
2. All requests for amendments will be made by having the client complete an "*Amendment of Health Record Request Form.*" The form will be forwarded to the Placer County Privacy Officer for documentation and processing.
3. Placer County is not obligated to agree to an amendment and may deny the requests or limit its agreement to amend.
4. If the request for amendment is granted, the County must:
 - 4.1. Append or otherwise provide a link to the location of the amendment;
 - 4.2. Provide the information to other entities and Business Associates that have the *Protected Health Information*, as well as to those entities as requested by the client;
 - 4.3. Notify the client in writing that the amendment is accepted and confirm to whom the amendment will be sent.

Grounds for denial of request for amendment:

- 4.4. The information to be amended was not created by the County (unless client provides reasonable basis to believe originator is no longer available).
- 4.5. The information to be amended is not part of the designated record.
- 4.6. The information to be amended would not otherwise be accessible to the client.
- 4.7. The client's record is complete and accurate.
5. If the request for amendment is denied or limited, the County must give the client a written statement in plain language, which must include:
 - 5.1. Advise the basis for denial (as listed above 5.1 – 5.4);
 - 5.2. Advise the client that he/she may submit a written statement of disagreement, to which the County may provide a rebuttal – all of which becomes part of the record for future disclosures. The advisement must also indicate that if the client declines to submit a written statement of disagreement, he/she may ask that his/her request for amendment and the denial be included with all future disclosures.
 - 5.3. Information on the County's complaint process.
6. The County must respond to the request no later than 60 days after the request is received. This may be extended no more than 30 days by providing the client (within the first 60 days) with a written reason for the delay and the date the County will comply.
7. If the County receives notice of an amendment from another covered entity, the information will be immediately incorporated into the record as indicated.

Form(s):

- *“Amendment of Health Record Request Form”*

Reference(s):

- *45 CFR Part 164.522 – 164.528*

Contact(s):

- Placer County HIPAA Privacy Officer. See main internal HHS web page, HIPAA contact page on County website, and current Placer County Telephone Directory for contact information.



HIPAA PRIVACY POLICIES

COUNTY OF PLACER

Policy Title:	Accounting of Disclosures		
Policy Number:	009	Version:	3.0
Approved By:	Placer County HIPAA Privacy Officer/Board of Supervisors		
Effective Date:	September 1, 2004. Revised October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or a Placer County HIPAA Hybrid Business Associate-like Entity.		

Purpose:

To describe the right that Placer County clients have regarding an accounting of disclosures of their **Protected Health Information**, and to describe the circumstances under which accountings are not required.

Definition:

For Definitions applicable to this and all HIPAA Privacy Policies, see the Definitions section of HIPAA Privacy Policy 001, "Definitions; Uses and Disclosures of Protected Health Information; Authorizations".

Policy:

Placer County clients have the right to receive an accounting of disclosures the County has made of their **Protected Health Information** for up to six years prior to the date of requesting such accounting. Information may not be available prior to April 14, 2003 and certain limitations apply as outlined in this Policy.

1. **Rights of clients to an accounting of disclosures of *Protected Health Information*:**

- 1.1. Clients have the right to receive an accounting of disclosures of **Protected Health Information** that the County has made for any period of time, not to exceed six years, preceding the date of requesting the accounting.
- 1.2. The accounting will only include **Protected Health Information** NOT previously authorized by the client for use or disclosure, and will not include information collected, used or disclosed for treatment, payment or health care operations for that client.
- 1.3. Clients may request a summary of disclosures by completing an "**Accounting of Disclosures Request Form**".

- 1.4. Personal representatives of the client also have the right to receive an accounting unless the County, in the exercise of professional judgment, believes that doing so would not be in the best interest of the client because of potential domestic violence, abuse, neglect, or otherwise endangering the client.
2. **The following disclosures will be tracked for accounting purposes:**
 - 2.1. Disclosures required by law (such as those involving abuse, domestic violence, communicable diseases, reportable injuries, Workers' Compensation, health oversight, and law enforcement).
 - 2.2. Disclosures for which an *Authorization* or opportunity to agree or object is not required.
 - 2.3. Disclosures for judicial or administrative proceedings (including responses to subpoenas and Court Orders).
 - 2.4. Disclosures made for research, unless previously authorized. In cases involving numerous records (50+) when an Independent Research Board or privacy board has waived requirement of client's *Authorization*, the County may meet the accounting requirement by summarizing the protocol and assisting the client in contacting the research sponsor if desired.
 - 2.5. Disclosure accountings may be temporarily suspended if requested by an oversight agency or law enforcement due to an ongoing investigation, if requesting entity provides a reasonable, specified time period in a written statement confirming that accounting may impede their case.
3. **The following disclosures do not have to be tracked or accounted for to the client:**
 - 3.1. Disclosures made for treatment, payment, or other health care operations.
 - 3.2. Disclosures made within the County for its own use.
 - 3.3. Disclosures authorized by the client or made directly to the client.
 - 3.4. Disclosures made for national security or intelligence purposes.
 - 3.5. Disclosures made to correctional institutions or law enforcement officials for inmates or those in police custody.
 - 3.6. Disclosures that delete identifying information.
 - 3.7. Disclosures that are not part of a limited data set.
 - 3.8. Disclosures that are incidental to another permitted use or disclosure.

Disclosures <u>Not Required</u> to Be Accounted	Disclosures <u>Required</u> to Be Accounted
For use in Treatment, Payment, or Health Care Operations	Communicable disease
Authorized by or made to the client	Abuse or domestic violence
For national security or intelligence purposes	Health Oversight
Correctional institutions or law enforcement regarding those individuals in custody	Law Enforcement
De-identified information	Subpoenas and Court Orders
Not part of a limited data set	Reportable injuries & Workers' Comp. investigations
Incidental to another permitted use or disclosure	Research
Disclosures made prior to April 14, 2003	
Re-disclosures by a non-County organization	

The first accounting in any 12-month period will be provided at no charge to the client. The client will be advised that subsequent requests during the same 12-month period will be charged at the rates set in County Code.

The County must respond to the request no later than 60 days after the request is received. This may be extended no more than 30 days by providing the client (within the first 60 days) with a written reason for the delay and the date the County will comply.

Content of the Accounting:

The Privacy Officer must prepare the content of an accounting as follows:

The Privacy Officer will determine the period of accounting, which will be covered in the accounting. Patients may request an accounting of disclosures made during any period of time falling within six years before the date of the request.

When preparing an accounting, the following information must be included for each disclosure:

- The date of the disclosure;
- The name of the person or organization that received the information;
- The address of the person or organization that received the information (if known);
- A brief description of the protected health information disclosed (with dates of treatment when possible); and
- At least one of the following items –
 - A brief statement explaining the purpose of the disclosure and why the disclosure is permitted under Placer County's policies, *or*
 - A copy of a written request made by a person or organization to whom the disclosure was made where the information was disclosed for one of the public policy reasons.

Documentation relating to a patient's request for an accounting must be maintained by Placer County for six years from the date of their creation.

Form:

- *“Accounting of Disclosures Request Form”*

Reference(s):

- *45 CFR Part 164.522 – 164.528*

Contact:

- Placer County HIPAA Privacy Officer. See main internal HHS web page, HIPAA contact page on County website, and current Placer County Telephone Directory for contact information.



HIPAA PRIVACY POLICIES

COUNTY OF PLACER

Policy Title:	Administrative, Technical, and Physical Safeguards Policy		
Policy Number:	010	Version:	2.0
Approved By:	Placer County HIPAA Privacy Officer/Board of Supervisors		
Effective Date:	September 1, 2004. Revised October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or a Placer County HIPAA Hybrid Business Associate-like Entity.		

Purpose:

To establish criteria for safeguarding confidential information and to minimize the risk of unauthorized or inadvertent access, use, or disclosures.

Definition:

For Definitions applicable to this and all HIPAA Privacy Policies, see the Definitions section of HIPAA Privacy Policy 001, "Definitions; Uses and Disclosures of Protected Health Information; Authorizations".

Policy:

1. General

Placer County will take reasonable steps to safeguard information from any intentional or unintentional use or disclosure that is in violation of the County's Privacy Policies. Information to be safeguarded may be in any medium, including paper, electronic, oral and visual representations of confidential information.

2. Safeguarding confidential information – County workplace practices

2.1. Paper – County staff assigned to workplaces that maintain **Protected Health Information** on paper will:

2.1.1. Store files and documents in locked rooms or storage systems.

2.1.2. Where lockable storage is not available, County staff must take reasonable efforts to ensure the safeguarding of confidential information.

2.1.3. Ensure that files and documents awaiting disposal or destruction in desk-site containers, storage rooms, or centralized waste/shred bins, are appropriately labeled, are shredded on a regular basis, and that all reasonable measures are taken to minimize access.

- 2.1.4. Ensure that shredding of files and documents is performed on a timely basis, consistent with record retention requirements.
- 2.1.5. In each County workplace, staff should be identified and documented who may have access to the information in order to perform their assigned duties.
- 2.1.6. If an employee is not the intended recipient of the information, it should not be read, but rather, returned to the sender or given to appropriate departmental authority for safekeeping and return.

2.2. Oral

- 2.2.1. County staff must take reasonable steps to protect the privacy of all verbal exchanges or discussions of **Protected Health Information**, regardless of where the discussion occurs.
- 2.2.2. Each County workplace that regularly serves as a location where **Protected Health Information** is verbally exchanged shall have enclosed offices and/or interview rooms available for such exchanges.

Exception: In work environments structured with few offices or closed rooms such as facilities with open office environments, uses or disclosures that are incidental to an otherwise permitted use or disclosure could occur. Such incidental uses or disclosures are not considered a violation, provided that the County has met the reasonable safeguards and minimum necessary requirements.

- 2.2.3. Each County workplace that serves as a location where **Protected Health Information** is verbally exchanged must foster employee awareness of the potential for inadvertent verbal disclosure of confidential information. Employees are expected to be aware of their surroundings and converse quietly to avoid unnecessary verbal disclosures.

2.3. Visual:

- 2.3.1. County staff must ensure that observable **Protected Health Information** is adequately shielded from unauthorized disclosure on computer screens and paper documents.
 - (a) Computer screens: Each County workplace that serves as a location where **Protected Health Information** is maintained must make every effort to ensure that confidential information on computer screens is not visible to unauthorized persons. This also applies to fax machines and printers. Employees should not leave any of these items unattended when communications are occurring.
 - (b) Paper documents: County staff must be aware of the risks regarding how paper documents are used and handled, and must take all necessary precautions to safeguard confidential information.

3. Safeguarding confidential information – County administrative safeguards

3.1. Implementation of role-based access and the *Minimum Necessary Policy* will promote administrative safeguards.

3.1.1. *Role Based Access (RBA)* is a form of security allowing access to data based on job function in accordance with County security procedures. Employees shall be assigned to an RBA group that will give members access only to the *Minimum Necessary* information to fulfill their job functions.

3.2. Conducting internal reviews periodically will permit Placer County to evaluate the effectiveness of safeguards.

3.2.1. County managers and supervisors will use the *County Safeguards Assessment Tool* to conduct annual reviews in order to evaluate and improve the effectiveness of their current safeguards.

3.3. Development and implementation of Countywide security policies will enhance administrative safeguards.

3.3.1. County staff will be required to sign a document that constitutes a formal commitment to adhere to the Countywide security policies.

Attachment(s):

- *Guidance for County Managers & Supervisors*
- *County Safeguards Assessment Tool*

Contact(s):

- Placer County HIPAA Privacy Officer. See main internal HHS web page, HIPAA contact page on County website, and current Placer County Telephone Directory for contact information.



HIPAA PRIVACY POLICIES

COUNTY OF PLACER

Policy Title:	Multi-Disciplinary Teams		
Policy Number:	011	Version:	2.0
Approved By:	Placer County HIPAA Privacy Officer/Board of Supervisors		
Effective Date:	September 1, 2004. Revised October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or a Placer County HIPAA Hybrid Business Associate-like Entity.		

Purpose:

To describe the parameters and responsibilities that Placer County staff have regarding the use and disclosure of *Protected Health Information* when participating in multi-disciplinary teams (MDTs).

Definitions:

For Definitions applicable to this and all HIPAA Privacy Policies, see the Definitions section of HIPAA Privacy Policy 001, "Definitions; Uses and Disclosures of Protected Health Information; Authorizations".

MDT -- Usually a team of two or more persons trained and qualified to address a common goal. In some cases that will be to identify the educational, health, social services needs of a child/family and develop a plan to address those needs. In other cases, it may be a team engaged in the prevention, identification and control of child abuse, premature death, juvenile crime, gang activity, elder or dependent adult abuse, sexual abuse or domestic violence.

An MDT that shares *Protected Health Information* may include, but is not limited to, representatives from social services, mental health, physical health, education, law enforcement, substance abuse treatment, child care agencies, prosecutors, probation, counselors and specialists in the particular area being discussed.

Policy:

Placer County staff may share *Protected Health Information* verbally during MDT meetings in order to better coordinate and integrate behavioral, social, physical health, and/or mental health care.

1. Information to be shared must be limited to data relevant to the intended purpose and function of the team and may not be further disseminated.
2. If required by law, staff must obtain the client's consent for multi-agency collaboration pursuant to a valid *Authorization*. The single *Authorization* must be written in plain language and must give a knowing and informed consent. Such a team would be a ***childrens multidisciplinary services team*** engaged in selecting appropriate integrated services for a particular family.
3. The signed *Authorization* must be retained for at least seven (7) years from its date of creation, or the date when it was last in effect, whichever is later. The agency responsible for maintaining the original *Authorization* is the lead agency handling the case, in which the client chart or record resides.
4. Such *Authorizations* are **NOT** required for multi-disciplinary teams engaged in the general prevention, identification, and treatment of:
 - Child abuse,
 - Juvenile crime,
 - Gang activity, or
 - Elder or dependent abuse.

In Placer County, this applies, but is not limited to:

- Sexual Assault Response Team (SART),
 - Multidisciplinary Interview Center (MDIC) Team,
 - Death Review Team,
 - Juvenile Justice Multidisciplinary Task Force,
 - Elder Abuse Task Force, and
 - Community Agency Multidisciplinary Elder Team (CAMET).
5. In all cases, each team participant, upon signing in at each meeting, acknowledges a confidentiality oath that the information to be shared is relevant to the intended purpose of the team and will not be further disseminated.
 6. No accounting of disclosures made in the context of the MDT is required.
 7. The MDT facilitator must assure that team members are fully trained in maintaining the confidentiality of any individually identifiable records.

Form(s):

- “*Authorization for Multi-Disciplinary Team Collaboration*”

Reference(s):

- 45 CFR Part 164.508
- Cal. Welfare & Institutions Code §§ 830, 830.1, 10850.1, 15633, 15754, 18964, 18986.40
- Cal. Health & Safety Code § 123145

Contact(s):

- Placer County HIPAA Privacy Officer. See main internal HHS web page, HIPAA contact page on County website, and current Placer County Telephone Directory for contact information.



HIPAA PRIVACY POLICIES

COUNTY OF PLACER

Policy Title:	Business Associate Relationships		
Policy Number:	012	Version:	3.0
Approved By:	Placer County HIPAA Privacy Officer/Board of Supervisors		
Effective Date:	September 1, 2004. Revised October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or a Placer County HIPAA Hybrid Business Associate-like Entity.		

Purpose:

The *HIPAA Privacy Rule* identifies a new category of business relationship, called a "***Business Associate***." The purpose of this Policy is to specify when Placer County may disclose an individual's ***Protected Health Information*** to a ***Business Associate*** of the County, and to specify what responsibilities County employees have with respect to ***Business Associates***.

Definition:

For Definitions applicable to this and all HIPAA Privacy Policies, see the Definitions section of HIPAA Privacy Policy 001, "Definitions; Uses and Disclosures of Protected Health Information; Authorizations".

Policy:

1. General

- 1.1. Placer County has many contractual and business relationships, and the County has policies related to its contracts and business relationships. However, not all contractors or business partners are "***Business Associates***" of Placer County. This Policy only applies to contractors or business partners that come within the definition of a "***Business Associate***".
- 1.2. If a contractor or business partner is a "***Business Associate***," those contracts that define the contractual relationship remain subject to all Federal and State laws and policies governing the contractual relationship. A "***Business Associate***" relationship also requires additional contract provisions that comply with 45 CFR 164.314.

1.3. **"Business Associate"** means:

1.3.1. With respect to Placer County, a person who:

- (a) On behalf of the County, but other than in the capacity of a County employee, performs or assists in the performance of:
 - (1) A function or activity involving the use or disclosure of Individually Identifiable Health Information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing benefit management, practice management, and re-pricing; or
 - (2) Any other function or activity regulated by Federal privacy regulations; or
 - (3) Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for Placer County, where the service involves disclosure of Individually Identifiable Health Information from the County, or from another **Business Associate** of the County.

1.4. A Covered Entity participating in an organized health care arrangement that performs a function or activity as described in (a)(1) of this definition or that provides a service as described in (a)(2) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a **Business Associate** of other Covered Entities participating in such organized health care arrangement. The status is dependent upon what the contractor does, not who they are.

1.5. A Covered Entity may be a **Business Associate** of another Covered Entity.

1.6. A **Business Associate** relationship is formed only if **Protected Health Information** is to be used, created, or disclosed in the relationship.

1.7. The following are **not Business Associates** or **Business Associate** relationships:

- 1.7.1. County employees, departments, divisions, and programs identified under the County's Hybrid Entity designation as covered entities or as business associate-like entities;
- 1.7.2. Medical providers providing treatment to individuals;
- 1.7.3. Enrollment or eligibility determinations, involving County clients, between government agencies;
- 1.7.4. County payment transactions to entities when the entity is providing its own normal services that are not on behalf of the County;
- 1.7.5. When an individual's **Protected Health Information** is disclosed based solely upon an individual's **Authorization**;
- 1.7.6. When an individual's **Protected Health Information** is not being disclosed by the County or created for the County; and

- 1.7.7. When the only information being disclosed is information that is de-identified in accordance with Placer County Policy, "***De-identification of Client or Participant Information and Use of Limited Data Sets.***"
- 1.8. Placer County may disclose an individual's ***Protected Health Information*** to a ***Business Associate*** and may allow a ***Business Associate*** to create or receive an individual's ***Protected Health Information*** on behalf of the County, if:
 - 1.8.1. Placer County first enters into a written contract, or other written agreement or arrangement that complies with 45 CFR 164.314, with the ***Business Associate*** before disclosing an individual's ***Protected Health Information*** to the ***Business Associate***, in accordance with the requirements of Section 2, below, of this Policy.
 - 1.8.2. The written contract or agreement provides satisfactory assurance that the ***Business Associate*** will appropriately safeguard the information and is signed by the appropriate parties before the person or entity performs any service that involves the use or disclosure of ***Protected Health Information***.
 - 1.8.3. If our ***Business Associate*** discloses health information to a **subcontractor or vendor**, the ***Business Associate*** must have a written contract that complies with 45 CFR 164.314 to ensure that the subcontractor or vendor also protects the privacy of the information.
2. Responsibilities of Placer County employees in ***Business Associate*** relationships:
 - 2.1. Be able to identify a ***Business Associate***; and
 - 2.2. Report any potential violations to the Privacy Officer & Contracts Administrator.
 - 2.3. When in doubt if a violation may have occurred, consult both the Privacy Officer and the Contracts Administrator.
3. ***Business Associate non-compliance***
 - 3.1. If Placer County knows of a pattern of activity or practice of a ***Business Associate*** that constitutes a material breach or violation of the ***Business Associate's*** obligation under the contract or other arrangement, the County must take reasonable steps to cure the breach or end the violation, as applicable, including working with and providing consultation to the ***Business Associate***.
 - 3.2. If mitigation efforts are unsuccessful, the Privacy Officer and staff will request that the County terminate the contract or arrangement. If not possible, the violation will be reported to the U.S. Department of Health and Human Services.

Reference(s):

- 45 CFR 160 & 164

Contact(s):

- Placer County HIPAA Privacy Officer. See main internal HHS web page, HIPAA contact page on County website, and current Placer County Telephone Directory for contact information.



HIPAA PRIVACY POLICIES

COUNTY OF PLACER

Policy Title:	De-identification of Client Information and Use of Limited Data Sets		
Policy Number:	013	Version:	2.0
Approved By:	Placer County HIPAA Privacy Officer/Board of Supervisors		
Effective Date:	September 1, 2004. Revised October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or a Placer County HIPAA Hybrid Business Associate-like Entity.		

Purpose:

To prescribe standards under which client information can be used and disclosed if information that can identify a person has been removed or restricted to a limited data set.

Definition:

For Definitions applicable to this and all HIPAA Privacy Policies, see the Definitions section of HIPAA Privacy Policy 001, "Definitions; Uses and Disclosures of Protected Health Information; Authorizations".

Policy:

1. General

- 1.1. Health information that does not identify an individual and for which there is no reasonable basis to believe that the information can be used to identify an individual will not be treated as ***Protected Health Information***.
- 1.2. De-identified information is client information from which Placer County or another entity has deleted, redacted, or blocked identifiers, so that the remaining information cannot reasonably be used to identify a person.
- 1.3. Unless otherwise restricted or prohibited by other Federal or State law, Placer County can use and share information as appropriate for the work of the County, without further restriction, if the County or another entity has taken steps to de-identify the information consistent with the requirements and restrictions of this policy in Section 2.
- 1.4. Placer County may use or disclose a limited data set that meets the requirements of Section 4 of this Policy, if the County enters into a ***Data Use Agreement*** with the limited data set recipient (or with the data source, if the County will be the

recipient of the limited data set) in accordance with the requirements of Section 5 of this Policy.

- 1.5. Placer County may disclose a limited data set only for the purposes of research, or non-governmental public health purposes. However, unless the County has obtained a limited data set that is subject to a *Data Use Agreement*, the County is not restricted to using a limited data set for its own activities or operations.
- 1.6. If Placer County knows of a pattern or activity or practice of the limited data set recipient that constitutes a material breach or violation of a *Data Use Agreement*, the County will take reasonable steps to cure the breach or end the violation and, if such steps are unsuccessful, the County will discontinue disclosure of information to the recipient and report the problem to the U.S. Department of Health and Human Services, Office for Civil Rights.

2. Requirements for de-identification of client information

2.1. Placer County may determine that client information is sufficiently de-identified, and cannot be used to identify an individual, only if **either** 2.1.1 or 2.1.2 below have occurred:

2.1.1. A statistician or other person with appropriate knowledge of, and experience with, generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

- (a) Has applied such principles and methods, and determined that the risk is minimal that the information could be used, alone or in combination with other reasonably available information, by a recipient of the information to identify the person whose information is being used; and
- (b) Has documented the methods and results of the analysis that justify such a determination; or

2.1.2. Placer County has ensured that:

(a) The following identifiers of the individual or of relatives, employers, and household members of the individual are removed:

- Names;
- All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geo codes. However, the initial three digits of a zip code may remain on the information if, according to current publicly-available data from the Bureau of the Census, the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and the initial three digits for all such geographic unit containing 20,000 or fewer people is changed to 000;
- All elements of dates (except year) for dates directly relating to an individual, including birth date, dates of admission and discharge

from a health care facility, and date of death. For persons age 90 and older, all elements of dates (including year) that would indicate such age must be removed, except that such ages and elements may be aggregated into a single category of "age 90 or older;"

- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social Security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate or license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including fingerprints and voiceprints;
- Full face photographic images and any comparable images, and
- Any other unique identifying number, characteristic, or codes, except as permitted under Section 3, below, of this policy; **and**

2.2. Placer County has no actual knowledge that the information could be used alone or in combination with other information to identify an individual who is the subject of the information.

2.3. The Privacy Officer will designate the statistician or other person referred to in subsection 2.1.1 above, who may be either:

2.3.1. A Placer County employee;

2.3.2. An employee of another governmental agency; or

2.3.3. An outside contractor or consultant, subject to County contracting and personnel policy.

3. Re-identification of de-identified information

3.1. Placer County may assign a code or other means of record identification to allow information de-identified under this policy to be re-identified by the County, except that:

- 3.1.1. The code or other means of record identification is not derived from or related to information about the individual and cannot otherwise be translated to identify the individual; and
- 3.1.2. Placer County does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

4. Requirements for a limited data set

- 4.1. A limited data set is information that excludes the following direct identifiers of the individual, or of relatives, employers or household members of the individual:
 - 4.1.1. Names;
 - 4.1.2. Postal address information, other than town or city, State and zip code;
 - 4.1.3. Telephone numbers;
 - 4.1.4. Fax numbers;
 - 4.1.5. Electronic mail addresses;
 - 4.1.6. Social Security numbers;
 - 4.1.7. Medical record numbers;
 - 4.1.8. Health plan beneficiary numbers (such as Medi-Cal Numbers);
 - 4.1.9. Account numbers;
 - 4.1.10. Certificate/license numbers;
 - 4.1.11. Vehicle identifiers and serial numbers, including license plate numbers;
 - 4.1.12. Web Universal Resource Locators (URLs);
 - 4.1.13. Internet Protocol (IP) address numbers;
 - 4.1.14. Biometric identifiers, including finger and voice prints; and
 - 4.1.15. Full face photographic images and any comparable images.

5. Contents of a Data Use Agreement

- 5.1. Placer County may disclose a limited data set only if the entity receiving the limited data set enters into a written *Agreement* with the County, in accordance with subsection 5.2 below, that such entity will use or disclose the *Protected Health Information* only as specified in the written *Agreement*.
- 5.2. A *Data Use Agreement* between Placer County and the recipient of the limited data set must:
 - 5.2.1. Specify the permitted uses and disclosures of such information by the limited data set recipient. Placer County may not use the *Agreement* to authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of this Policy if done by the County.

- 5.2.2. Specify who is permitted to use or receive the limited data set; and
- 5.2.3. Specify that the limited data set recipient will:
- (a) Not use or further disclose the information other than as specified in the *Data Use Agreement* or as otherwise required by law;
 - (b) Use appropriate safeguards to prevent use or disclosure of the information other than as specified in the *Data Use Agreement*;
 - (c) Report to Placer County, if the County is the source of the limited data set, if the recipient becomes aware of any use or disclosure of the information not specified in its *Data Use Agreement* with the County;
 - (d) Ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and
 - (e) Not identify the information or contact the individuals whose data is being disclosed.

Reference(s):

- 45 CFR 164.514

Contact(s):

- Placer County HIPAA Privacy Officer. See main internal HHS web page, HIPAA contact page on County website, and current Placer County Telephone Directory for contact information.



HIPAA PRIVACY POLICIES

COUNTY OF PLACER

Policy Title:	Enforcement, Sanctions, and Penalties for Violations of Individual Privacy		
Policy Number:	014	Version:	2.0
Approved By:	Placer County HIPAA Privacy Officer/Board of Supervisors		
Effective Date:	September 1, 2004. Revised October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or a Placer County HIPAA Hybrid Business Associate-like Entity.		

Purpose:

To specify enforcement, sanction, penalty, and disciplinary actions that may result from violations of County policies regarding the privacy and protection of an individual's **Protected Health Information** and any other legally protected information.

Definition:

For Definitions applicable to this and all HIPAA Privacy Policies, see the Definitions section of HIPAA Privacy Policy 001, "Definitions; Uses and Disclosures of Protected Health Information; Authorizations".

Policy:

1. General

- 1.1. All employees, volunteers, interns and members of the Placer County workforce must guard against improper uses or disclosures of a County client or participant's **Protected Health Information**.
 - 1.1.1. County employees, volunteers, interns and members of the workforce who are uncertain if a disclosure is permitted are advised to consult with a supervisor. The Privacy Officer is a resource for any unresolved disclosure question, and may be consulted in accordance with County operational procedures.
- 1.2. All employees who may have access to **Protected Health Information** are required to be aware of their responsibilities under County Privacy Policies.
 - 1.2.1. County employees will be expected to sign a "**Statement of Understanding**," indicating that they have been informed of County business practices as they relate to privacy, and they understand their

responsibilities to ensure the health privacy of County clients and participants.

- 1.3. Supervisors are responsible for assuring that employees who have access to confidential information, whether it be electronic, hard copy, or orally, are informed of their responsibilities.
- 1.4. Sanctions for using or disclosing PHI in violation of HIPAA or County Policies or Procedures regarding HIPAA will be imposed in accordance with Placer County's discipline policy, up to and including termination. Documentation of sanctions will be retained for a minimum of five years.
- 1.5. County employees who knowingly and willfully violate State or Federal law for improper use or disclosure of an individual's **Protected Health Information** are subject to criminal investigation and prosecution or civil monetary penalties.
- 1.6. If Placer County fails to enforce privacy safeguards, the County may be subject to administrative penalties by the State of California and/or the U.S. Department of Health and Human Services, including monetary penalties.

2. Retaliation prohibited

- 2.1. Neither Placer County as an entity nor any County employee will intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against:
 - 2.1.1. Any individual for exercising any right established under County policy, or for participating in any process established under County policy, including the filing of a complaint with the County, the State of California, or with the U.S. Department of Health and Human Services.
 - 2.1.2. Any individual or other person for:
 - (a) Filing of a complaint with the County, the State of California, or with the U.S. Department of Health and Human Services as provided in County privacy policies;
 - (b) Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing relating to County privacy policies and procedures; or
 - (c) Opposing any unlawful act or practice, provided that:
 - (1) The individual or other person (including a County employee) has a good faith belief that the act or practice being opposed is unlawful; and
 - (2) The manner of such opposition is reasonable and does not involve a use or disclosure of an individual's **Protected Health Information** in violation of County policy.

3. Disclosures by whistleblowers and workforce crime victims

3.1. A County employee or Business Associate may disclose an individual's *Protected Health Information* if:

3.1.1. The County employee or Business Associate believes, in good faith, that the County has engaged in conduct that is unlawful or that otherwise violates professional standards or County policy, or that the care, services, or conditions provided by the County could endanger County staff, persons in County care, or the public; **and**

3.1.2. The disclosure is to:

- (a) An oversight agency or public authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of Placer County;
- (b) An appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or of misconduct by Placer County; or
- (c) An attorney retained by or on behalf of the County employee or Business Associate for the purpose of determining the legal options of the County employee or Business Associate with regard to this County policy.

3.2. A Placer County employee may disclose limited *Protected Health Information* about an individual to a law enforcement official if the employee is the victim of a criminal act and the disclosure is about only the suspected perpetrator of the criminal act.

Form(s):

- *"Statement of Understanding"*

Reference(s):

- 45 CFR 164.530
- *Confidentiality of Medical Information Act, Cal. Civ. Code § 56-56.16*

Contact(s):

- Placer County HIPAA Privacy Officer. See main internal HHS web page, HIPAA contact page on County website, and current Placer County Telephone Directory for contact information.



HIPAA PRIVACY POLICIES

COUNTY OF PLACER

Policy Title:	<i>Uses and Disclosures for Research Purposes & Waivers</i>		
Policy Number:	015	Version:	2.0
Approved By:	Placer County HIPAA Privacy Officer/Board of Supervisors		
Effective Date:	September 1, 2004. Revised October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or a Placer County HIPAA Hybrid Business Associate-like Entity.		

Purpose:

To specify when Placer County may use or disclose information about individuals for research purposes.

Definition:

For Definitions applicable to this and all HIPAA Privacy Policies, see the Definitions section of HIPAA Privacy Policy 001, "Definitions; Uses and Disclosures of Protected Health Information; Authorizations".

Policy:

1. General

When Placer County uses or discloses an individual's information for research purposes, it must consider the following:

- 1.1. Placer County may use or disclose an individual's information for research purposes as specified in this policy. "Research" means "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge."
- 1.2. All such research disclosures are subject to applicable requirements of State and Federal laws and regulations and to the specific requirements of this Policy.

Note: This Policy is intended to supplement existing research requirements of the *Common Rule, 45 CFR Part 46*. The *Common Rule* is the rule for the protection of human subjects in research promulgated by the U.S. Department of Health and Human Services, and adopted by other Federal governmental agencies, including the National Institutes for Health, for research funded by those agencies. In addition, some agencies have

requirements that supplement the *Common Rule* that are applicable to a particular research contract or grant.

- 1.3. De-identified information may be used or disclosed for purposes of research, consistent with Placer County Policy, "*De-identification of Client Information and Use of Limited Data Sets.*"
- 1.4. A limited data set may be used or disclosed for purposes of research, consistent with the policies related to Limited Data Sets in Placer County Policy, "*De-identification of Client Information and Use of Limited Data Sets.*"
- 1.5. Placer County may also conduct public health studies, studies that are required by law, and studies or analysis related to its health care operations. Such studies will be discussed in Sections 4 and 5 of this Policy.

2. Institutional Review Board (IRB) or Privacy Board established by Placer County

Placer County may use an IRB established in accordance with *45 CFR Part 46* or a Privacy Board that has been established by the County pursuant to this Policy, to perform the duties and functions specified in this Policy regarding a research project being conducted, in whole or in part, by the County or by a County department, division, or program.

3. Uses and disclosures for research purposes – specific requirements

3.1. Placer County may use or disclose client or participant information for research purposes with the client's specific written *Authorization*.

3.1.1. Such *Authorization* must meet all the requirements described in Placer County Policy, "*Uses and Disclosures of Client or Participant Information.*"

3.1.2. An *Authorization* for use and disclosure for a research study may be combined with any other type of written permission for the same research study.

3.1.3. If research includes treatment, the researcher may condition the provision of research related treatment on the provision of an *Authorization* for use and disclosure for such research.

3.2. Placer County may use or disclose client or participant information for research purposes without the client's or participant's written authorization provided that:

3.2.1. The County obtains documentation that a waiver of an individual's *Authorization for Release of Information* requirements has been approved by either:

(a) An Institutional Review Board (IRB); or

(b) A Privacy Board that:

(1) Has members with varying backgrounds and appropriate professional competency as needed to review the effect of the

research protocol on the individual's privacy rights and related concerns;

- (2) Includes at least one member who is not affiliated with Placer County, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any such entity; and
- (3) Does not have any member participating in a review of any project in which the member has a conflict-of-interest.

3.2.2. Documentation required of IRB or Privacy Board when granting approval of a waiver of an individual's *Authorization for Release of Information* must include:

- (a) A statement identifying the IRB or Privacy Board that approved the waiver of an individual's *Authorization*, and the date of such approval;
- (b) A statement that the IRB or Privacy Board has determined that the waiver of *Authorization*, in whole or in part, satisfies the following criteria:
 - (1) The use or disclosure of an individual's *Protected Health Information* involves no more than minimal risk to the privacy of individuals, based upon at least the following elements:
 - (i) An adequate plan to protect an individual's identifying information from improper use or disclosure;
 - (ii) An adequate plan to destroy an individual's identifying information at the earliest opportunity, consistent with the conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
 - (iii) Adequate written assurances that the *Protected Health Information* will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of the *Protected Health Information* would be permitted under this Policy;
 - (2) The research could not practicably be conducted without the waiver; and
 - (3) The research could not practicably be conducted without access to and use of the individual's *Protected Health Information*;
- (c) A brief description of the *Protected Health Information* for which use or disclosure has been determined to be necessary by the IRB or Privacy Board;

- (d) A statement that the waiver of an individual's *Authorization* has been reviewed and approved under either normal or expedited review procedures, by either an IRB or a Privacy Board, pursuant to Federal regulations at *45 CFR 164.512(2)*; and
- (e) The Privacy Board Chair must sign documentation of the waiver of an individual's *Authorization*, or other member as designated by the Chair of the IRB or the Privacy Board, as applicable.

3.2.3. In some cases, a researcher may request access to individual information maintained by Placer County in preparation for research or to facilitate the development of a research protocol in anticipation of research. Before agreeing to provide such access to individual information, Placer County should determine whether Federal or State law otherwise permits such use or disclosure without individual authorization or use of an IRB. If there is any doubt whether the use and disclosure of the information by the researcher falls within this *HIPAA* exception, review by an IRB or Privacy Board and formal waiver of *Authorization* is required. If such access falls within this *HIPAA* exception to authorization and is otherwise permitted by other Federal or State law, Placer County will only provide such access if the County obtains, from the researcher, written representations that:

- (a) Use or disclosure is sought solely to review an individual's protected information needed to prepare a research protocol or for similar purposes to prepare for the research project;
- (b) No client information will be removed from Placer County by the researcher in the course of the review; the client information for which use or access is sought is necessary for the research purposes;
- (c) Researcher and his or her agents agree not to use or further disclose the information other than as provided in the written Agreement, and to use appropriate safeguards to prevent the use or disclosure of the information other than is provided for by the written Agreement;
- (d) Researcher and his or her agents agree not to publicly identify the information or contact the individual whose data is being disclosed; and
- (e) Applicable Federal or State law may require such other terms or conditions.

3.2.4. In some cases, a researcher may request access to *Protected Health Information* maintained by Placer County about individuals who are deceased. The County should determine whether Federal or State law otherwise permits such use or disclosure of information about decedents without individual authorization or use of an IRB. There may be instances where it would be inappropriate to disclose information, even where the individual subject of the information is dead – for example, individuals who died of AIDS may not have wanted such information to be disclosed after

their deaths. If there is any doubt whether the use and disclosure of the information by the researcher falls within this *HIPAA* exception, review by an IRB or Privacy Board and formal waiver of authorization is required. If such access falls within this *HIPAA* exception to authorization and is otherwise permitted by other Federal or State law, Placer County will only provide such access if the County obtains the following written representations from the researcher:

- (a) Representation that the use or disclosure is sought solely for research on the *Protected Health Information* of deceased persons;
- (b) Documentation, if the County so requests, of the death of such persons; and
- (c) Representation that the individual's *Protected Health Information* for which use or disclosure is sought is necessary for the research purposes.
- (d) Researcher and his or her agents agree not to use or further disclose the information other than as provided in the written Agreement, and to use appropriate safeguards to prevent the use or disclosure of the information other than is provided for by the written Agreement;
- (e) Researcher and his or her agents agree not to publicly identify the information or contact the personal representative or family members of the decedent; and
- (f) Applicable Federal or State law may require such other terms or conditions.

4. **Placer County Public Health Studies and Studies Required by Law**

When Placer County is operating as a Public Health Authority, the County is authorized to obtain and use individual *Protected Health Information* without authorization for the purpose of preventing injury or controlling disease and for the conduct of public health surveillance, investigations and interventions. In addition to these responsibilities, Placer County may collect, use or disclose information, without individual authorization, to the extent that such collection, use or disclosure is required by law. When the County uses information to conduct studies pursuant to such authority, no additional individual authorization is required nor does this Policy require IRB or Privacy Board waiver of authorization based on the *HIPAA Privacy Rule*. Other applicable laws and protocols continue to apply to such studies.

5. **Placer County Studies Related to Health Care Operations**

Studies and data analyses conducted for Placer County's own quality assurance purposes and to comply with reporting requirements applicable to Federal or State funding requirements fall within the uses and disclosures that may be made without individual authorization as Placer County health care operations. Neither individual authorization nor IRB or Privacy Board waiver of authorization is required for studies

or data analyses conducted by or on behalf of the County for purposes of health care operations, including any studies or analyses conducted to comply with reporting requirements applicable to Federal or State funding requirements. "Health care operations" as defined in *45 CFR 164.501* include:

- 5.1. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities;
- 5.2. Conducting population-based activities relating to improving health care or reducing health care costs, protocol development, case management and care coordination, contacting health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
- 5.3. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, and conducting training programs, and accreditation, certification, licensing or credentialing activities;
- 5.4. Underwriting, premium rating, and other activities related to the creation, renewal or replacement of a contract of health insurance or health benefits;
- 5.5. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
- 5.6. Business planning and development, such as conducting cost-management and planning related analyses related to managing and operating Placer County, including improvement of administration or development or improvement of methods of payment or coverage policies; and
- 5.7. Business management and general administrative activities of Placer County, including management activities related to *HIPAA* implementation and compliance; customer services, including the provision of data analyses for policy holders, plan sponsors, or other customers; resolution of internal grievances; and
- 5.8. Creating de-identified information or a limited data set consistent with the Placer County Policy, "*De-identification of Client Information and Use of Limited Data Sets.*"
- 5.9. **Exception:** HIV-AIDS information may not be disclosed to anyone without the specific written authorization of the individual. Re-disclosure of HIV test information is prohibited, except in compliance with law or with written permission from the individual.

Reference(s):

- *45 CFR Part 64*
- *45 CFR 164.501, 164.506*

Contact(s):

- Placer County HIPAA Privacy Officer. See main internal HHS web page, HIPAA contact page on County website, and current Placer County Telephone Directory for contact information.



HIPAA PRIVACY POLICIES

COUNTY OF PLACER

Policy Title:	Policy and Procedure for Notification of a Breach of Unsecured <i>Protected Health Information</i>		
Policy Number:	016	Version:	2.0
Approved By:	Placer County HIPAA Privacy Officer/Board of Supervisors		
Effective Date:	September 23, 2013. Revised October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or a Placer County HIPAA Hybrid Business-Associate like Entity.		

Purpose:

Placer County Dept. of Health and Human Services (“Placer County”) and its contractors and vendors will strive to prevent breaches of Unsecured Protected Health Information (“PHI”) and personal information (“PI”) electronically or otherwise, and maintain privacy and security measures to protect the confidentiality of PHI and PI.

Placer County has implemented reasonable and appropriate Administrative, Physical and Technical Safeguards to protect the confidentiality, integrity and availability of PHI and PI in its possession.

Placer County has implemented reasonable systems for the discovery and reporting of a breach of PHI or PI.

This policy describes the process by which Placer County will notify individuals regarding a confirmed breach of security when Unsecured PHI has been acquired, assessed, used or disclosed by an unauthorized person.

Definitions:

For Definitions applicable to this and all HIPAA Privacy Policies, see the Definitions section of HIPAA Privacy Policy 001, "Definitions; Uses and Disclosures of Protected Health Information; Authorizations".

A “*breach*” of PHI is the unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of the PHI.

Policy:

Pursuant to the Health Insurance Portability and Accountability Act (“HIPAA”) and Regulations promulgated thereunder, Placer County will notify individuals when Unsecured *Protected Health Information (PHI)* has been acquired, accessed, used or disclosed by an unauthorized person, when a confirmed breach of the security of the system does not fall within a statutory exception or there is not a low probability that the PHI has been compromised.

Confirmed breaches of the security or privacy of Unsecured PHI will invoke certain actions to determine the probability that the PHI has been compromised based on a risk assessment and, under specific circumstances, notification of the breach will be made to the affected individual(s).

Procedure:

1. When a breach has been reported or suspected, the suspected breach will immediately be reported to the HIPAA Privacy Officer and/or Security Officer, and an investigation into the breach will be conducted.
2. The investigation and steps taken will be thoroughly documented. If the conclusion of the investigation is that no breach occurred, no further action is necessary, but the investigation and conclusion will be thoroughly documented.
3. If it is confirmed that a breach of security or confidentiality has occurred and has resulted in the unauthorized disclosure of PHI, the following risk assessment steps will be taken:
 - 3.1. Determine whether or not the information breached was Unsecured. Unsecured PHI includes information not secured through encryption or destruction, and is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary of the Department of Health and Human Services (“HHS”) in guidance issued under Section 13402(h)(c) of Public Law 111-5.
 - 3.2. Determine the reasonable likelihood that such information was accessed by an unauthorized person.
 - 3.3. Determine the probability that the PHI has been compromised based on a risk assessment of at least the following factors: (i) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (ii) the unauthorized person who used the PHI or to whom the disclosure was made; (iii) whether the PHI was actually acquired or viewed; and (iv) the extent to which the risk to the PHI has been mitigated.
4. The risk assessment will be documented thoroughly, including the actions taken, the conclusions of the assessment and the basis for the determination that there was or was not a low probability that the PHI was compromised.
5. If it is determined that the information breached was secured and there is no reasonable likelihood that the secured information was rendered usable, readable or

viewable by an unauthorized person, no further action is necessary, but the determination and conclusion will be documented.

6. If it is determined that the information breached was Unsecured, but the circumstance of the breach falls within one of the exceptions to HIPAA (45 C.F.R. § 164.42), so notification is not required, such determination will be documented.
7. If it is determined that the breach of the security of the system demonstrates that there is more than a low probability that the PHI was compromised, Placer County will as soon as possible, but no later than 60 days after the discovery of the breach, notify the individual(s) whose information was disclosed as a result of the breach, and the determination and conclusion will be documented.
8. If it is determined that the information breached was Unsecured and notification is required, an analysis of the requirements for notification of the State in which the individuals reside will be conducted and documented, including Cal. Civ. Code § 1798.80 and Cal. Health & Safety Code. § 1280.15.
9. If notification to law enforcement or another regulatory body or agency is required under State law, such notification will be made to the regulatory body or agency in accordance with State law.
10. If State law requires notification to the individual, notification will be made in accordance with State law, including Cal. Civ. Code § 1798.80 and Cal. Health & Safety Code. § 1280.15.
11. Notification to the individual may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and the notification will be made after law enforcement determines it will not compromise its investigation.
12. Notification of a breach to affected individuals will be in plain language and include at a minimum:
 - 12.1. a brief description of what happened, including the date of the breach and discovery of the breach;
 - 12.2. a description of the type of Unsecured PHI or other personal information that was involved in the breach;
 - 12.3. any steps individuals should take to protect themselves from potential harm resulting from the breach;
 - 12.4. a description of the investigation into the breach, mitigation of harm to individuals, and protection against further breaches; and
 - 12.5. contact procedures, which will include a toll-free telephone number, an e-mail address, website or postal address.
13. The notification must include any additional information required by applicable State law, including Cal. Civ. Code § 1798.80 and Cal. Health & Safety Code. § 1280.15.
14. If the breach involves more than 500 residents of a state or jurisdiction, notice will be provided to the media and to the Secretary of HHS contemporaneously.

15. A log of any and all breaches of Unsecured PHI of less than 500 individuals will be maintained and reported to the Secretary of HHS on an annual basis.
16. Business Associates and vendors, through their contracts and/or Business Associate Agreements with Placer County will be required to provide notification of a breach to Placer County so affected individuals can be notified, as necessary. Business Associates must provide all available information without delay.
17. Documentation will be maintained of each individual notified, each notification provided to HHS and any other notification to the Secretary of HHS as required by law.
18. If required to notify under the California State breach notification law, Cal. Civ. Code § 1798.80, if unencrypted PI was or is reasonably believed to have been acquired by an unauthorized person, the breach notification required under this State law shall include, but will not limited be to, the following:
 - 18.1. The name and contact information of the reporting person or business.
 - 18.2. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - 18.3. If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.
 - 18.4. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
 - 18.5. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
 - 18.6. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.
19. If more than 500 California residents require notification, notification to the California Attorney General will also be provided.
20. If required to notify under the California Health & Safety Code § 1280.15, due to the unlawful or unauthorized access to, and use or disclosure of, an individual's medical information, notice will be provided no later than five (5) business days after the discovery of such access, use or disclosure.

Form:

- ***“Health Information Privacy Complaint”***
- ***“Breach Report and Investigation Form”***

Reference(s):

- *HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414*
- *§ 13407 of the HITECH Act*

Contact:

- Placer County HIPAA Privacy Officer. See main internal HHS web page, HIPAA contact page on County website, and current Placer County Telephone Directory for contact information.



HIPAA PRIVACY POLICIES

COUNTY OF PLACER

Policy Title:	Privacy Policy		
Policy Number:	017	Version:	2.0
Approved By:	Placer County HIPAA Privacy Officer/Board of Supervisors		
Effective Date:	September 23, 2013. Revised October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or a Placer County HIPAA Hybrid Business Associate-like Entity.		

1. Introduction

Placer County Dept. of Health and Human Services ("Placer County") hereby implements this Privacy Policy pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH") with respect to its activities when receiving protected health information ("PHI").

Placer County is designated as a "hybrid entity" in accordance with 45 CFR § 164.105, as it performs both covered as well as non-covered component functions as part of its business operations. Members of Placer County's workforce employed within functions determined to be covered entities or business associate-like entities under the hybrid designation may have access to PHI as defined by HIPAA.

It is Placer County's policy to comply with HIPAA's requirements for the privacy of PHI. To that end, all Placer County's hybrid entity Workforce Members who have access to PHI must comply with this Privacy Policy.

No third-party rights are intended to be created by this Policy. Placer County reserves the right to amend or change this Policy at any time (and even retroactively) without notice. To the extent this Policy establishes requirements and obligations above and beyond those required by HIPAA or HITECH the Policy shall be aspirational and shall not be binding upon Placer County. To the extent this Policy is in conflict with the HIPAA Privacy Rule, the HIPAA Privacy Rule shall govern.

Definition:

For Definitions applicable to this and all HIPAA Privacy Policies, see the Definitions section of HIPAA Privacy Policy 001, "Definitions; Uses and Disclosures of Protected Health Information; Authorizations".

2. Placer County's Responsibilities as a Covered Entity

2.1. Privacy Officer and Contact Person

The Director of Health & Human Services has been authorized by the Board of Supervisors to appoint the Privacy Officer for Placer County. The Privacy Officer will be responsible for the development and implementation of policies and procedures relating to privacy of PHI in the possession of Placer County, including but not limited to this Privacy Policy. The Privacy Officer will also serve as the contact person for individuals who have questions, concerns, or complaints about the privacy of PHI.

The Privacy Officer is responsible for ensuring that Placer County complies with the provisions of the HIPAA Privacy Rule regarding third-party business associate vendors or subcontractors, including the requirement that a HIPAA-compliant Business Associate Agreement is in place with business associate vendors or subcontractors of Placer County. The Privacy Officer shall also be responsible for monitoring compliance with the HIPAA Privacy Rule and this Privacy Policy.

2.2. Workforce Training

It is Placer County's policy to train all Workforce Members who have access to PHI on Placer County's HIPAA Policy and Procedures. The Privacy Officer is charged with developing training schedules and programs so that all Workforce Members receive the training necessary and appropriate to permit them to carry out Placer County's functions in compliance with HIPAA and HITECH.

2.3. Safeguards and Firewall

Placer County will establish appropriate administrative, technical, and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements. Placer County has implemented HIPAA Security Policies that set forth the security measures in place to protect the privacy of PHI.

2.4. Complaints

The Privacy Officer will be Placer County's contact person for receiving complaints.

The Privacy Officer is responsible for creating a process for individuals to lodge complaints about the Plan's privacy procedures and for creating a system for handling such complaints. A copy of the complaint procedure shall be provided to any participant upon request.

2.5. Sanctions for Violations of Privacy Policy

Placer County will apply appropriate sanctions against Workforce Members who fail to comply with the security policies and procedures of the County's covered entity as described in the policy section of the Placer County *HIPAA Policy 014, "Enforcement, Sanctions, and Penalties for Violations of Individual Privacy."*

2.6. Mitigation of Inadvertent Disclosures of PHI

Placer County shall mitigate, to the extent possible, any harmful effects that become known to it from a use or disclosure of an individual's PHI in violation of HIPAA or the policies and procedures set forth in this Policy. As a result, if an Workforce Member or business associate vendor or subcontractor becomes aware of an unauthorized use or disclosure of PHI, either by an employee or a business associate vendor or subcontractor, the Workforce Member or business associate vendor or subcontractor must immediately contact the Privacy Officer so that appropriate steps to mitigate harm to the client can be taken.

2.7. No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy

No Workforce Member may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA.

2.8. Documentation

Placer County's privacy policies and procedures shall be documented and maintained for at least six years from the date last in effect. Policies and procedures must be changed as necessary or appropriate to comply with changes in the law, standards, requirements and implementation specifications (including changes and modifications in regulations). Any changes to policies or procedures must be promptly documented.

The documentation of any policies and procedures, actions, activities and designations may be maintained in either written or electronic form. Placer County will maintain such documentation for at least six years.

2.9. Workforce Must Comply With Placer County's Policy and Procedures

Placer County's Workforce Members who have access to PHI must comply with this Policy.

2.10. Breach Notification Requirements

Placer County will comply with the requirements of the HITECH Act and its implementing regulations to provide notification to affected individuals, HHS, and the media (when required) if Placer County or one of its business associate vendors or subcontractors discovers a breach of unsecured PHI.

2.11. Mandatory Disclosures of PHI

PHI must be disclosed in the following situations:

- The disclosure is to the individual who is the subject of the information;
- The disclosure is required by law; or
- The disclosure is made to the HIPAA Privacy Officer, HIPAA Security Officer, County Counsel, or other HHS HIPAA consultant for purposes of implementing or enforcing HIPAA.

2.12. Other Permitted Disclosures of PHI

PHI may be disclosed in the following situations without the client's authorization, when specific requirements are satisfied. The requirements include prior approval of the Privacy Officer. Permitted are disclosures —

- about victims of abuse, neglect or domestic violence;
- for treatment purposes;
- for judicial and administrative proceedings;
- for law enforcement purposes;
- for public health activities;
- for health oversight activities;
- about decedents;
- for cadaveric organ-, eye- or tissue-donation purposes;
- for certain limited research purposes;
- to avert a serious threat to health or safety;
- for specialized government functions; and
- that relate to workers' compensation programs.

2.13. Disclosure of Sensitive Information

Except as provided in section 2.11, at no time may a client's sensitive information, including HIV/AIDS, drug and/or alcohol, genetic, mental health, sexually transmitted diseases or family planning be disclosed without the client's consent.

2.14. Complying With the "Minimum Necessary" Standard

To the extent practicable, Placer County will limit its use and/or disclosure of PHI to a Limited Data Set. A Limited Data Set is PHI that excludes the

following identifiers of the individual or of relatives, employers, or household members of the individual:

- (i) Names;
- (ii) Postal address information, other than town or city, State, and zip code;
- (iii) Telephone numbers;
- (iv) Fax numbers;
- (iv) Electronic mail addresses;
- (v) Social Security numbers;
- (vi) Medical record numbers;
- (vii) Health plan beneficiary numbers;
- (ix) Account numbers;
- (x) Certificate/license numbers;
- (xi) Vehicle identifiers and serial numbers, including license plate numbers;
- (xii) Device identifiers and serial numbers;
- (xiii) Web Universal Resource Locators (URLs);
- (xiv) Internet Protocol (IP) address numbers;
- (xv) Biometric identifiers, including finger and voice prints; and
- (xvi) Full face photographic images and any comparable images.

If it is not practicable for Placer County to limit its use and/or disclosure of PHI to a Limited Data Set, Placer County will use the "minimum necessary" PHI to accomplish the purpose of the use or disclosure.

Minimum Necessary When Disclosing PHI. Placer County, when disclosing PHI subject to the minimum necessary standard, shall take reasonable and appropriate steps to ensure that only the minimum amount of PHI that is necessary for the requestor is disclosed. All disclosures not discussed in this Policy must be reviewed on an individual basis with the Privacy Officer to ensure that the

amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

Minimum Necessary When Requesting PHI. Placer County, when requesting PHI subject to the minimum necessary standard, shall take reasonable and appropriate steps to ensure that only the minimum amount of PHI necessary for Placer County is requested. All requests must be reviewed on an individual basis with the Privacy Officer to ensure that the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.

2.15. Disclosures of PHI to Business Associates

Workforce Members may disclose PHI to Placer County's business associate vendors or subcontractors and allow Placer County's business associate vendors or subcontractors to create or receive PHI on its behalf. However, prior to doing so, Placer County must first obtain assurances from the business associate vendor or subcontractor that it will appropriately safeguard the information. Before sharing PHI with outside consultants or contractors who meet the definition of a "business associate," Workforce Members must contact the Privacy Officer and verify that a Business Associate Agreement is in place.

2.16. Disclosures of De-Identified Information

Placer County may freely use and disclose information that has been "de-identified" in accordance with the HIPAA Privacy Rule.

2.17. Accounting

An individual has the right to obtain an accounting and an Access Report of certain access and disclosures of his or her own PHI. This right to an accounting extends to disclosures made in the last six years, except for disclosures of electronic disclosures of Electronic Health Records (EHRs), for which the right to an accounting extends:

- to carry out treatment, payment, or health care operations (except in the case of EHRs, for which this exception does not apply);
- to individuals about their own PHI;
- incident to an otherwise permitted use or disclosure;
- pursuant to an authorization;
- to persons involved in the individual's care or payment for the individual's care or for certain other notification purposes;
- to correctional institutions or law enforcement when the disclosure was permitted without authorization;
- as part of a limited data set;
- for specific national security or law enforcement purposes; or
- disclosures that occurred prior to the compliance date.

Placer County shall respond to an accounting request within 60 days. If Placer County is unable to provide the accounting within 60 days, it may extend the period by 30 days, provided that it gives the participant notice (including the reason for the delay and the date the information will be provided) within the original 60-day period.

The accounting must include the date of the disclosure, the name of the receiving party, a brief description of the information disclosed, and a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure (or a copy of the written request for disclosure, if any). If a brief purpose statement is included in the accounting, it must be sufficient to reasonably inform the individual of the basis of the disclosure.

The first accounting in any 12-month period shall be provided free of charge. The Privacy Officer may impose reasonable production and mailing costs for subsequent accountings.

Forms:

- *“Health Information Privacy Complaint”*
- *“Authorization for Release of Information”*
- *“Accounting of Disclosures Request”*
- *“Statement of Understanding/Training Acknowledgement”*

Reference(s):

- *HIPAA Privacy Rule, 45 CFR Part 160 & Subparts A and E of Part 164*

Contact:

- Placer County HIPAA Privacy Officer. See main internal HHS web page, HIPAA contact page on County website, and current Placer County Telephone Directory for contact information.



HIPAA PRIVACY POLICIES

COUNTY OF PLACER

Policy Title:	Client Request for Additional Privacy Protections		
Policy Number:	018	Version:	2.0
Approved By:	Placer County HIPAA Privacy Officer/ Board of Supervisors		
Effective Date:	September 1, 2004. Revised October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or a Placer County HIPAA Hybrid Business Associate-like Entity.		

PURPOSE:

From time to time, clients may request certain additional privacy protections for their health information. For example, clients may request restrictions on the way Placer County uses and discloses their protected health information. They may also request that we communicate with them by an alternative means or method that is more confidential for them. It is Placer County's policy to respond to all client requests in a respectful manner. Under the law, special procedures must be followed when handling such requests. **Clients requesting additional privacy protections should therefore be directed to submit their requests to the Privacy Officer.**

Definition:

For Definitions applicable to this and all HIPAA Privacy Policies, see the Definitions section of HIPAA Privacy Policy 001, "Definitions; Uses and Disclosures of Protected Health Information; Authorizations".

IMPLEMENTATION OF POLICY:

The following procedures should be followed in response to client requests for additional privacy protections.

1. Refer the Client to the Privacy Officer

If a client requests additional privacy protections, Placer County Workforce Members should direct the client to submit his or her request to the Privacy Officer, who is the only person authorized to grant or deny the requests. *Placer County Workforce Members should never grant a client's request, nor provide any assurances that the request will be granted, unless the Privacy Officer has specifically approved the request.* The client's request for additional privacy protections should never be denied

outright by a Workforce Member without requesting that the client submit his or her request to the Privacy Officer.

2. Compliance with Notices Placing Restrictions on Use and Disclosure of Information

2.1. Ordinary Circumstances

All Placer County Workforce Members are expected to review a client's medical record for possible restrictions on the use or disclosure of the client's information. Restrictions will be posted in the appropriate section of the client's medical record. All restrictions must be followed.

2.2. Emergency Circumstances

In rare situations, Placer County Workforce Members may ignore a restriction if *absolutely necessary* to provide the client with emergency treatment. The Privacy Officer must be consulted if a restriction must be ignored in order to provide emergency treatment to a client. The Privacy Officer will document his or her reasons in the client's medical record. If restricted protected health information is disclosed to another health care provider to facilitate emergency treatment, the health care provider will be advised not to further use or disclose the information beyond what is necessary to provide the emergency treatment.

2.3. Terminating Restrictions

Client's Initiative

A client may request that a restriction be modified or terminated at any time. The client must submit his or her request to terminate the restriction in writing to the Privacy Officer. If there is insufficient time to obtain a written request, a Workforce Member may accept the client's oral request, which must then be recorded in the client's medical record as soon as possible. A Workforce Member must notify the Privacy Officer of an oral request as soon as possible after the request is made. Only the Privacy Officer may approve modification or termination of a restriction.

Placer County's Initiative

Placer County may also initiate modification or termination of a restriction at any time.

Notice and Documentation

The Privacy Officer will inform the client of any modifications to, or terminations of, additional privacy restrictions previously granted. The Privacy Officer will be responsible for documenting that any modifications and terminations are included in the client's record.

3. Compliance With Notices Requiring Confidential Communications

All Workforce Members are expected to review a client's medical record for possible notices requiring that the client be contacted by an alternative method that is more confidential for the client. These notices will be posted in the appropriate section of the client's medical record.

VIOLATIONS:

Workforce Members who violate this policy will be subject to disciplinary action up to and including termination of employment or contract with Placer County.

Contact :

- Placer County HIPAA Privacy Officer. See main internal HHS web page, HIPAA contact page on County website, and current Placer County Telephone Directory for contact information.



HIPAA PRIVACY POLICIES

COUNTY OF PLACER

Policy Title:	Policy and Procedure for HIPAA and HITECH Documentation		
Policy Number:	019	Version:	2.0
Approved By:	Placer County HIPAA Privacy Officer/Board of Supervisors		
Effective Date:	September 23, 2013. Revised October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or a Placer County HIPAA Hybrid Business Associate-like Entity.		

Purpose:

This policy is designed to give guidance for compliance with provisions of the Health Insurance Portability and Accountability Act (HIPAA) of 1996, the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) and implementing regulations requiring covered entities to maintain documentation of policies, procedures and other administrative documents.

Definition:

For Definitions applicable to this and all HIPAA Privacy Policies, see the Definitions section of HIPAA Privacy Policy 001, "Definitions; Uses and Disclosures of Protected Health Information; Authorizations".

Policy:

1. Placer County Dept. of Health and Human Services ("Placer County") will implement policies and procedures with respect to protected health information ("PHI") designed to comply with the standards, implementation specifications, or other requirements of the HIPAA Privacy regulations.
2. Placer County will maintain documentation, in written or electronic form, of policies, procedures, communications, and other administrative documents as required by 45 C.F.R §164.530 (i) and (j), for a period of at least six years from the date of creation or the date when last in effect, whichever is later.
3. Placer County will incorporate any changes in law into its policies, procedures, and other administrative documents, as necessary.

Procedures:

1. Placer County's policies have been reasonably designed to take into account the size and type of activities undertaken by the organization with respect to PHI.

2. The following documentation will be maintained in an organized manner:
- Policies and procedures related to the use or disclosure of PHI;
 - Policies and procedures related to sanctions for a violation of policies and procedures;
 - Policies and procedures related to requests of individuals for an accounting of disclosures and Access Report;
 - Requests for the use or disclosure of PHI;
 - Policies and procedures related to minimum necessary disclosure;
 - Policies and procedures related to fundraising and marketing of PHI.

Reference(s):

- *45 CFR §164.530 (i) and (j)*

Contact:

- Placer County HIPAA Privacy Officer. See main internal HHS web page, HIPAA contact page on County website, and current Placer County Telephone Directory for contact information.



HIPAA PRIVACY POLICIES

COUNTY OF PLACER

Policy Title:	Uses and Disclosures of <i>Protected Health Information</i> for Marketing Activities		
Policy Number:	020	Version:	2.0
Approved By:	Placer County HIPAA Privacy Officer/Board of Supervisors		
Effective Date:	September 23, 2013. Revised October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or a Placer County HIPAA Hybrid Business Associate-like Entity.		

Definition:

For Definitions applicable to this and all HIPAA Privacy Policies, see the Definitions section of HIPAA Privacy Policy 001, "Definitions; Uses and Disclosures of Protected Health Information; Authorizations".

Policy:

Placer County marketing activities involving the use or disclosure of protected health information may only be conducted after being approved by the Placer County HIPAA Privacy Officer and authorized marketing staff at Placer County who will ensure that requirements set forth in the Health Insurance Portability and Accountability Act ("HIPAA") of 1996 and the Health Information Technology for Economic and Clinical Health Act ("HITECH") for the use and disclosure of client information have been met. Client information or lists should not be used or released before this approval has been obtained from authorized marketing staff, as there are legal restrictions on marketing activities of Placer County.

If Placer County receives financial remuneration from a third party in exchange for client information, an authorization from the client is required including an acknowledgement that remuneration is being received. Financial remuneration means direct or indirect payment from or on behalf of a third party whose product or service is being described, not including payment for client treatment.

Implementation:

1. Marketing Activities Subject to this Policy

Marketing activities generally include all oral or written communications with a client about a product or service that encourage the client to purchase or use that product or service. Placer County marketing activities may involve client information because the marketing is directed at current or former clients. Marketing also may include distributing client information to another organization so that it may market its own products and services if Placer County receives direct or indirect payment in exchange for the client information.

2. Marketing Activities Not Subject to this Policy

Marketing activities not subject to this policy include:

2.1. Refill reminders or other drugs or biologics currently prescribed to a client if any financial remuneration received by Placer County in exchange for making the communication is reasonably related to Placer County's cost of making the communication;

2.2. Treatment and health care operations purposes where Placer County does not receive financial remuneration in exchange for making the communication, including:

2.2.1. Treatment by a health care provider;

2.2.2. Case management or care coordination;

2.2.3. Recommendations for alternative treatments, therapies, providers or settings of care;

2.2.4. Descriptions of a health related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of Placer County, including communications about Placer County participation in a health care provider or health plan network, replacements and/or enhancements to health plans or health-related products or services available to a health plan enrollee that add value to, but are not part of, their plan or benefits.

3. Responsibility

It is the responsibility of Placer County's Privacy Officer to implement processes to ensure that the distribution of marketing materials adhere to this policy, HIPAA, and HITECH.

4. Approval

To obtain approval for marketing activities contact the Privacy Officer.

Violations:

Placer County's Privacy Officer has general responsibility for implementation of this policy. Anyone who violates this policy will be subject to disciplinary action up to and including termination of employment or contract with Placer County. Anyone who knows or has reason to believe that another person has violated this policy should report the matter promptly to Placer County's Privacy Officer. Any attempt to retaliate against a person for reporting a violation of this policy will itself be considered a violation of this policy that may result in disciplinary action up to and including termination of employment or contract with Placer County.

Reference(s):

- *HIPAA, 45 CFR 164.501, 164.508(a)(3)*

Contact:

- Placer County HIPAA Privacy Officer. See main internal HHS web page, HIPAA contact page on County website, and current Placer County Telephone Directory for contact information.



HIPAA PRIVACY POLICIES

COUNTY OF PLACER

Policy Title:	Uses and Disclosures of <i>Protected Health Information</i> for Fundraising Activities		
Policy Number:	021	Version:	2.0
Approved By:	Placer County HIPAA Privacy Officer/Board of Supervisors		
Effective Date:	September 23, 2013. Revised October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or a Placer County HIPAA Hybrid Business Associate-like Entity.		

Definition:

For Definitions applicable to this and all HIPAA Privacy Policies, see the Definitions section of HIPAA Privacy Policy 001, "Definitions; Uses and Disclosures of Protected Health Information; Authorizations".

Policy:

Fundraising activities involving the use or disclosure of client information may only be conducted by authorized development staff at Placer County, upon approval by the HIPAA Privacy Officer, who will ensure that all requirements for the use and disclosure of such information have been met. Fundraising communications may only be sent to individuals who have not opted out of receiving such communications. Placer County may not condition treatment or payment on the individual's choice with respect to receipt of fundraising communications.

Implementation:

1. Fundraising Activities Subject to this Policy

Fundraising activities include any activities undertaken to raise money, or other things of value, on behalf of Placer County or any of its affiliated organizations. This policy applies to any fundraising activities undertaken by Placer County, Placer County staff (including Placer County volunteers), Placer County vendors, subcontractors and other business associates. Examples of fundraising activities include:

- Requests for general donations to benefit Placer County;
- Requests for special-purpose donations;
- Requests for sponsorship of Placer County events or activities; and
- Auctions, rummage sales, or bake sales.

The fundraising activities are subject to this policy only if the activities involve the use or disclosure of client information. Placer County may use or disclose to a business associate or to an institutionally related foundation, ONLY the following client information for purposes of fundraising on its own behalf, without a client authorization:

- Name;
- Address;
- Other contact information;
- Age;
- Gender;
- Date of birth;
- Dates of health care provided;
- Department of service;
- Treating physician;
- Outcome information; and
- Health insurance status.

Sensitive health information including, but not limited to, HIV/AIDS, mental/behavioral health, sexually transmitted diseases, genetic testing, and substance abuse treatment information may not be disclosed for fundraising purposes.

2. Approval By Development Staff

To obtain approval of fundraising activities by Placer County's development staff, contact the Privacy Officer.

3. Opt-Out Requests

Individuals have the right to opt-out of receiving fundraising communications. All fundraising communications must contain clear and conspicuous language providing the individual the opportunity to opt-out of receiving fundraising communications without any undue burden or more than a nominal cost on the individual. All individuals' requests to opt out of such communications should be forwarded to authorized development staff.

It is the responsibility of the Privacy Officer in connection with the development office, to implement processes to ensure that individuals who have opted-out of receiving fundraising communications do not receive such communications. However, the individual may be provided the opportunity to opt back in to receive fundraising communications if they have previously elected to opt-out of such communications.

Violations:

Placer County's Privacy Officer has general responsibility for implementation of this policy. Anyone who violates this policy will be subject to disciplinary action up to and including termination of employment or contract with Placer County. Anyone who knows or has reason to believe that another person has violated this policy should report the matter promptly to his or her supervisor or Placer County's Privacy Officer. All reported matters will be investigated, and, where appropriate, steps will be taken to remedy the situation. Any attempt to retaliate against a person for reporting a violation of this policy will itself be considered a violation of this policy that may result in disciplinary action up to and including termination of employment or contract with Placer County.

Questions:

If you have questions about this policy, please contact Placer County's Privacy Officer immediately. It is important that all questions be resolved as soon as possible to ensure protected health information is used and disclosed appropriately.

Reference(s):

- *HIPAA, 45 CFR §164.514(f)*

Contact:

- Placer County HIPAA Privacy Officer. See main internal HHS web page, HIPAA contact page on County website, and current Placer County Telephone Directory for contact information.



HIPAA PRIVACY POLICIES

COUNTY OF PLACER

Policy Title:	Policy and Procedure on Compliance with Confidentiality and Non-Disclosure Agreement		
Policy Number:	022	Version:	2.0
Approved By:	Placer County HIPAA Privacy Officer/Board of Supervisors		
Effective Date:	September 23, 2013. Revised October 7, 2014		
Policy Applies To:	All Placer County employees assigned to work in a department or program formally designated as a Placer County HIPAA Hybrid Covered Entity or a Placer County HIPAA Hybrid Business Associate-like Entity.		

Definition:

For Definitions applicable to this and all HIPAA Privacy Policies, see the Definitions section of HIPAA Privacy Policy 001, "Definitions; Uses and Disclosures of Protected Health Information; Authorizations".

Procedure:

1. Only authorized users are granted access to PHI and PI. Such access is limited to specific, defined, documented and approved applications and level of access rights.
2. As a condition to receiving access rights to PHI and PI (either by electronic or hard copy access), each Workforce Member and user must agree, in writing, to comply with established terms and conditions. Failure to comply with such terms and conditions may result in the denial and/or immediate suspension of access to PHI and PI.
3. A violation of the terms of the confidentiality and non-disclosure agreement may be grounds for disciplinary action, including termination of employment or contract, loss of privileges, legal action for monetary damages and/or injunction, or any other remedy available to Placer County.

Form:

- *"Confidentiality and Non-Disclosure Agreement"*

Reference(s):

- *This Policy and Procedure is a County-specific document and is not required under a specific law or regulation*

Contact:

- Placer County HIPAA Privacy Officer. See main internal HHS web page, HIPAA contact page on County website, and current Placer County Telephone Directory for contact information.