County of Sacramento — Office of Compliance

HIPAA PRIVACY & SECURITY RULE TRAINING
TEMPORARY AGENCY, VOLUNTEERS, REGISTRY & CONTRACTORS
Health Insurance Portability and Accountability Act (HIPAA)

HIPAA Sets National Standards for:

- Privacy of confidential, protected health information (Protected Health Information = PHI)
- Security of health information – physical, technical and administrative security measures
- Electronic exchange of health information

How Does HIPAA Work With State Laws?

HIPAA creates a federal privacy floor (minimum requirement) and supersedes any contrary state law. State law governs if it is more stringent than HIPAA, providing greater privacy protections.

What is Protected Health Information–PHI (and ePHI)?

PHI is health information in any form or medium that identifies an individual, and relates to:

- The individual's past, present, or future physical or mental health condition;
- The provision of health care to the individual; or
- The past, present, or future payment for the provision of health care to the individual.

Electronic Protected Health Information (ePHI) is health information that a HIPAA covered entity creates or receives in electronic (computer) media and/or is maintained in any form of electronic media:

- Computer files, email, electronic medical records
- Shared network drives for HIPAA covered programs
- Laptop computers, CDs, USB drives, smartphones, tablets, or any portable electronic device

The HIPAA Privacy and Security Rules Apply Only to Covered Entities (and Business Associates):

This training concentrates on the County of Sacramento's HIPAA-covered workforce.

- **Health care providers** who electronically transmit health information

  Examples: Physicians, hospitals, labs, public health departments

  (Excludes providers who submit transactions on paper)

- **Health plans** who provide or pay the cost of medical care

  Examples: Medicaid, Medicare, Blue Cross

HIPAA **excludes** Workers' Compensation, Disability, WIC, and government-funded programs whose primary mission is not providing for or paying the cost of medical care.

The County is a HIPAA Covered Entity and a Hybrid:

A "hybrid entity" is a single entity whose business activities include both covered and non-covered functions and that designates its health care components. The hybrid entity is responsible for ensuring that its health care components comply with HIPAA.

What Does HIPAA address?

- When and how a covered entity (or business associate) may use or disclose **PHI and ePHI** - it sets boundaries on the use and disclosure of health records
- Individuals' rights respecting PHI and ePHI - gives clients more control over their health information
- Organizational requirements – what the County of Sacramento is required to do - establishes safeguards to protect privacy of health information
- Relationships between HIPAA covered entities and those not covered by HIPAA
- Civil and criminal penalties for HIPAA violations

What is "Covered Information" According to HIPAA?

All protected health information (PHI) held or disclosed by a covered entity (or business associate) in **any** form, whether in paper records, communicated orally, on computers or in other electronic format. PHI is found, for example, in medical records, billing records, insurance/benefit enrollment, case or medical management records, prescription fulfillment systems, etc.

PHI is medical information that is personally identifiable. Identifiers include the following:

Names, street addresses - city, county precinct, zip codes (all geographic subdivisions smaller than a state...All elements of dates (except year) including birth date, admission date, discharge date, date of death...Telephone numbers, fax numbers, Social Security numbers, medical records numbers, health plan beneficiary numbers, account numbers, vehicle identifiers and serial numbers, including license plate numbers, health plan beneficiary numbers… Email addresses, web site addresses (URLs), internet protocol (IP) addresses… Biometric identifiers, including finger and voice prints and full face photographic images or any comparable images of an individual.

PHI Does Not Include: Education records, Workman's Compensation records or health information in your personnel records. These records are not covered by HIPAA because they do not belong to HIPAA covered entities.

What is the Difference Between "Use" and "Disclosure" of PHI?

- **USE** - The ***sharing***, employment, application, utilization, examination, or analysis of protected health information (PHI) ***within*** (**inside**) the entity that maintains the PHI
- **DISCLOSURE** - The ***release***, transfer, provision of access to, or divulging in any other manner of PHI ***outside*** the entity holding the information

What are the HIPAA Rules About Use and Disclosure of PHI?

The County of Sacramento may only use or disclose PHI for *purposes permitted or required* and in *ways that are permitted or required* by HIPAA. A use or disclosure that is not permitted or required by the rule is prohibited by the law.

What Are Required Disclosures?

HIPAA requires disclosure of PHI in only two circumstances:

- Upon request by the individual who is the subject of the information
- When the Office for Civil Rights, under the direction of the Federal U.S. DHHS, investigates compliance or violations of privacy and security

What Are Permitted Uses *and* Disclosures?

- Uses and disclosures for treatment, payment, and health care operations (TPO)
- Uses and disclosures that require the individual's permission
- Those requiring an authorization
- Those where the individual must be given an opportunity to agree or object
- Certain limited uses and disclosures for important governmental purposes

What About Treatment, Payment and Operations (TPO)?

Under HIPAA, no authorization is required and a covered entity may use and disclose PHI:

- For its own TPO
- For treatment activities of any health care provider
- For payment activities of any health care provider
- For health care operations of another covered entity (under some circumstances)

Definition of Treatment: *Providing*, coordinating or managing health care; *coordinating* and *managing* health care by a health care provider with a third party; *consultations* among health care providers; *referrals* of patients from one health care provider to another

Definition of Payment: Obtaining premiums (not applicable to Medicaid) or fulfilling obligations for coverage and the provision of benefits (*example*: Medicaid eligibility); obtaining or providing reimbursement (*example*: Medicaid payment of claims).

A HIPAA covered entity may release PHI for payment purposes to non-covered organizations or components within its own organization (*example*: PHI may be disclosed to obtain reimbursement from a disability insurance carrier).

Definition of Health Care Operations: Administrative and business management activities of the covered entity. Some of these include: quality *assessment*; development of clinical guidelines; case management and care coordination; sharing information about treatment alternatives; competency and performance reviews; training programs; fraud and abuse detection, patient safety activities and compliance programs.

What Types of Use or Disclosure *Always* Require An Authorization?

Authorizations are required for disclosures of PHI for purposes other than TPO:

1. That are not otherwise allowed under the Privacy Rule
2. For disclosures to third parties specified by the client
3. To use or disclose psychotherapy notes

Authorizations may be initiated by the client or by the County of Sacramento (*examples*: Client wants PHI disclosed for life insurance application; client wants their PHI sent to their attorney; health care worker wants to help client apply for disability benefits).

What Does a County Authorization Form Have to Include?

When you fill out the County's HIPAA Form 2099 – "Authorization to Obtain or Release Medical Records" – the Form 2099 MUST include the following:

- A description of information to be used or disclosed that identifies the information in a specific, meaningful fashion (I: Discharge summary, laboratory reports, clinical reports, etc)
- The name (specific identification) of the person(s) authorized to request the use or disclosure
- The name (specific identification) of the person(s) to whom the covered health care component is making the requested use or disclosure (examples: Law firm of Smith and Jones, Johnson Corporation – Diabetes Research Project staff, etc.)
- The expiration date that relates to the client and purpose for use or disclosure (examples: 90 days from date authorization is signed; 30 days post discharge, etc.). County policy requires it must be less than one year.
- Description of each purpose of requested use or disclosure
- If authorization is client-initiated, it is sufficient to state "At the request of the individual"
- Signature of client or personal representative and date of the authorization
- Description of personal representative's authority to sign for client (*example*: guardian of person)
- Advise patients they can refuse to sign. The County may not condition treatment, payment, and/or enrollment in a health plan, or eligibility for benefits on signing of authorization by client *except*, A.) if the County is providing health care solely for purpose of creating PHI for disclosure to third party (*example*: life insurance physical) or B) prior to enrollment in a health plan if authorization is for eligibility or enrollment determinations.

When is an Authorization Form Invalid?

- When the expiration date has passed or expiration event is known to have occurred
- When it is not filled out completely with all required elements listed above
- When it is revoked by client

- When information in the authorization is known by component to be false
- When the authorization is combined with any other document

Can PHI be Disclosed to Family Members or Friends?

Yes, under certain circumstances, such as:

- Use or disclosure of PHI to notify or assist in notification of individual's location, or general condition is permitted if the individual is first given opportunity to agree or object. Verbal agreement is possible if the client is given opportunity to object to the disclosure and does not object or if you, as a health care provider, can reasonably conclude the client agrees (*example*: the client asks friend to remain during the medical exam).
- If client is not able to respond (*examples*: incapacitated, in an emergency situation or dead) *or* if the client is not present, the health care provider may use or disclose PHI directly relevant to person's involvement if, based upon professional judgment, disclosure is in the best interest of the client (*example*: a designated relative is picking up a prescription)

What Other Situations Do Not Require an Authorization to Use or Disclose?

Covered health care components may use or disclose PHI without an authorization under the following exceptions. **In every situation, do not release any information, and refer the request for use or disclosure to your supervisor.**

- **Activities involving Public Health** – No authorization is needed to release PHI to public health authorities who, by law, collect or receive PHI to prevent or control disease, injury, disability; or for public health surveillance, investigations, or interventions. Do not take action on any request for release of PHI to public health authorities without consulting your supervisor. There are specific procedures in each of the County's covered components for responding to these requests.

- **Child Abuse or Neglect** - To a government authority (*example*: Child Protective Services – CPS) authorized by law to receive reports of child abuse or neglect. Child abuse reporting is considered a "Public Health Activity". Do not take action on any report of child abuse or neglect. Immediately refer the matter to your supervisor for evaluation under state and federal laws as well as County policies and procedures.

- **Adult abuse, neglect, or domestic violence** – HIPAA covered health care components may disclose the victim's PHI in order to report abuse, neglect, or domestic violence (when required by law and necessary to prevent serious harm). Do not take action on any report of adult abuse, neglect or domestic violence without consulting your supervisor.

- **Health oversight activities -** PHI can be disclosed to public oversight agencies (and to private entities acting on behalf of public agencies) without client authorization for activities authorized by law such as: audits (*example*: Medicaid audits); civil, administrative, or criminal investigations; inspections and disciplinary. Do not take action on any release of PHI to public oversight agencies. Refer any such request to your immediate supervisor.

- **Judicial and administrative proceedings –** PHI may be released without authorization as required by law, such as State statutes and administrative codes; Federal law; court orders; court-ordered warrants; subpoenas, summons from a court, grand jury, discovery request or other lawful process. Do not take action on any request for release by a court order, subpoena, discovery request or other lawful process. Refer any such request to your immediate supervisor. There are specific procedures in each of the County's covered components for these legal/judicial requests.

- **Some limited law enforcement purposes –** A covered health care component may disclose **limited** PHI to law enforcement officials (LEO) as required by law. Do not take action on any request for release of PHI by law enforcement officials. Refer any such request to your immediate supervisor. There are specific procedures in each of the County's covered components for these law enforcement requests for disclosure of PHI, including reporting.

- **Decedents** – A covered health care component can disclose PHI to coroners and medical examiners for identification of a deceased person, determining cause of death or other duties authorized by law. PHI can be disclosed to funeral directors when it is consistent with applicable law, to carry out their duties w/respect to the decedent, prior to and in reasonable anticipation of death (*example*: pre-pay burial arrangement). A covered health care component may also disclose PHI about the deceased to LEO when there is suspicion that death may have resulted from criminal conduct. Do not take action on any request for release of PHI by a coroner, medical examiner or funeral director. Refer any such request to your immediate supervisor. There are specific procedures in each of the County's covered components for these requests for disclosure of PHI.

- **Serious threat to health or safety –** A covered health care component may, in good faith, use or disclose PHI when consistent with applicable law, and when, in good faith, it believes it is necessary to prevent or lessen serious and imminent threat to health or safety of a person (or public). There are specific limitations to the information that can be released. Do not take action on any release of PHI where a potential threat to health or safety may be identified. Immediately refer the matter to your immediate supervisor for evaluation under state and federal laws as well as County policies and procedures.

- **Other specialized government functions** – these include the following:

  Corrections and Lawful Custody. A covered health care component may disclose PHI to a correctional institution (prison, jail, reformatory, detention center, halfway house, residential community program center) or to LEO having lawful custody of inmate or other individual. An individual is no longer an inmate when released on parole, probation, supervised release, or no longer in lawful custody. Do not take action on any release of PHI regarding an individual in lawful custody. Refer the request to your supervisor for evaluation and direction.

  Government Programs providing Public Benefits. Covered health plans that are government programs providing public benefits may disclose PHI relating to eligibility or enrollment in the health plan to another agency administering a government program providing public benefits under certain conditions. Do not take action on any release of PHI in connection with providing public benefits. Refer the request to your supervisor for evaluation and direction.

- **Workers' Compensation -** Covered entity may disclose PHI in accordance with workers compensation. Workers compensation programs are not covered under HIPAA.

- **Employers – Public Health Activities -** No authorization is required to release PHI to an employer about a member of the workforce under certain conditions. The healthcare provider (County of Sacramento) must give written notice that PHI related to work-related illness, injury, or surveillance is disclosed to the employer. Do not take action on any request for release of PHI from an employer regarding a member of their workforce. Refer this immediately to your supervisor.

Are There Other Requirements About Use and Disclosure of PHI and ePHI?

The "MINIMUM NECESSARY" and "NEED TO KNOW" standards should apply in all your contacts with PHI and ePHI. Ask yourself these questions:

- Is it necessary for your job?
- How much do you need to know?
- How much do other people need to know?

How Does "Need to Know" Translate into HIPAA?

The HIPAA Privacy Rule states that a covered component may provide only the minimum necessary amount of PHI necessary:

- To accomplish the purpose for which use or disclosure is sought
- To those among the workforce who need the information to perform their job

Are There Exceptions to the "Minimum Necessary" Standard?

The Minimum Necessary standard does not apply to:

- Disclosure to or request by a health care provider for treatment purposes. (*However, the minimum necessary standard does apply to 'P' (payment) and 'O' (operations) of TPO*.)
- Disclosures to the client who is the subject of information. (*However, access to the client can be limited under certain conditions*.)
- Uses or disclosures authorized by client. (*However, only what is authorized may be disclosed*.)
- Uses or disclosures required by law
- Disclosures to U.S. DHHS for compliance/enforcement activities
- Uses or disclosures required for compliance with standard transactions (in connection with billing, etc.).

Are There Other Use and Disclosure Requirements?

For disclosures of PHI or ePHI, a covered health care component must always verify the identity of the person requesting the information and their authority to have access to the PHI. Make sure you're disclosing the correct individual's information, and check for restrictions.

What are the County's Requirements for Verifying Identity?

The identity of an individual should be verified with a **photo ID** such as a driver' license or state ID card **or two or more of the following**: military ID, military discharge papers, government employee badge, naturalization papers, immigration cards, certified copy of birth certificate, passport, check cashing card, food stamp ID card.

Always refer the request for release and verifying documents immediately to your supervisor.

What is a "Personal Representative"?

A "personal representative" is a person with authority to act on behalf of an individual in making decisions related to health care. General rule: treat a personal representative as if they were the individual. Limitation: the person is treated as a personal representative only with respect to PHI that is relevant to the personal representation. If the parent's last name is different from child's last name, determine relationship to child.

Before releasing health information about a minor child under the care of a guardian (or other person acting in place of the parent), request copies of guardianship papers and refer the request for disclosure to your supervisor for determination.

What are the Rights of Clients under HIPAA?

- Right to receive notification if their PHI is breached
- Right to file a Privacy complaint
- Right to request additional protections such as confidential communication, receiving PHI at alternate locations, by alternative means
- Right to access, inspect, and copy their own PHI with exception of psychotherapy notes or information compiled for legal proceeding
- Right to request to amendment or correction of their PHI
- Right to request and receive an accounting of disclosures of their PHI.
- Right to receive a Notice of Privacy Practices. The Notice must be posted prominently and must be available at time of service. You will be trained at your work site in the specific procedures used by your program.
- Right to request restrictions of use or disclosure of PHI. The County does not have a duty to agree to requests and will not agree to any restriction if it adversely affects the quality of the client's care or services or limits/prevents payment for services. Do not agree to any restrictions of use. Immediately refer client requests for any restrictions to your supervisor for action.

There are specific County HIPAA forms and department procedures used in implementing these client rights, as well as **strict response deadlines**. Immediately refer client requests under these categories to your supervisor for action.

Is the County Required to Track Disclosures of PHI and ePHI?

Yes, under HIPAA, covered health care components are required to track certain disclosures of protected health information and there is a specific HIPAA form to use (County Form 2097,

"Accounting of Disclosures"). Electronic Medical Records (EMRs) will use a format similar to the Accounting of Disclosures form that contains the information required by the Accounting of Disclosures. See below.

A client has a right to receive a written accounting of those disclosures of their PHI in the six years prior to the date on which the accounting was requested, but not going back before April 14, 2003 (when HIPAA was enacted).

Your supervisor will train you how to use the disclosure form at your work site, along with specific procedures from the department, division or program where you are placed.

What Information is Required in the Accounting of Disclosure?

The following content is required to be included in County HIPAA form 2097:

- Date of disclosure
- Name (and address, if known) of entity or person who received the PHI
- Brief description of the PHI disclosed
- Brief statement of disclosure's purpose
- Copy of written request for disclosure

Multiple disclosures to same entity/person have specific content requirements. **Refer any circumstance of multiple disclosures of this type to your immediate supervisor for guidance in correct documentation.**

What Disclosures Have to be Tracked?

The disclosures which must be included are those for:

- Public health activities, including communicable disease reporting
- Birth and death reporting
- Law enforcement in emergencies where a crime is suspected
- Judicial/administrative proceedings, response to a subpoena or discovery request
- Workers compensation purposes
- Medical examiners, funeral directors, coroners about decedents
- Adult or child abuse reporting
- Disclosures to a person who may have been exposed to a communicable disease
- Disclosures to law enforcement, for locating a suspect or fugitive
- Health oversight agencies

Not all disclosures require tracking. *Exceptions* are disclosures for:

- Treatment, payment or operations (TPO)
- To clients for their own PHI

- Facility directories
- National security or intelligence purposes
- Correctional institutions or law enforcement officials
- Those that occurred prior to April 14, 2003
- Incidental disclosures
- Those made with an authorization
- Persons involved in client's care

There are circumstances when the right for an accounting of disclosure may be temporarily suspended by request from health oversight agencies or law enforcement. **You will be trained by your supervisor on department, division or program procedure if this circumstance should arise in performance of your job.**

Are There Other HIPAA Requirements?

The County of Sacramento, as a HIPAA hybrid entity, must designate a Privacy Officer and a Security Officer, develop, implement and maintain written policies and procedures, train its workforce, establish procedures for receiving complaints, and report breaches of protected health information to the federal DHHS.

A covered health care component is also required to:

- Have in place appropriate administrative, technical and physical safeguards
- Safeguard PHI and ePHI from any intentional or unintentional use or disclosure
- Retain documentation for at least 6 years (The County retains HIPAA documentation for 7 years)
- Take reasonable steps to reduce, to the extent possible, any harmful effects of a violation of privacy policies and procedures or HIPAA requirements

Safeguards You Must Follow

- Use available safeguards to keep al protected health information private and secure
- Keep medical test results private
- Do NOT share PHI with unauthorized individuals or have it viewable in public areas
- Never share and always protect computer passwords
- Always return medical records to appropriate location
- Dispose of paper containing PHI properly in a locked shred bin
- Obtain supervisor knowledge and approval before sending PHI in email
- Email containing PHI that is sent outside the County network must be encrypted
- Obtain supervisor knowledge and approval before downloading data

- Mobile devices that contain ePHI must be secured with passwords and/or encryption and kept with you at all times
- Put medical records in a secure location where others cannot see them or access them to prevent unauthorized viewing and access
- Make sure copies of PHI at copy machines, printers, or fax machines are retrieved immediately
- Don't leave PHI exposed in mail boxes or conference rooms
- Always lock your computer when leaving the work area and log off when you are done for the day
- Secure PHI when no one is in the area, lock file cabinets and office doors
- Close doors or draw privacy curtains/screens
- Conduct discussions so that others may not overhear them
- If PHI or ePHI is taken off site take measures to secure the information. Treat it the same whether on site or offsite.

HIPAA Security Awareness – What is it?

- Recognizing what types of security issues may arise in the workplace, and
- Knowing what actions to take in the event of a security breach.

The Top 8 Workplace Security Mistakes:

1. Hidden under the keyboard – Keeping a computer password on a yellow post-it note
2. I'll do it my way – Not listening to or following security procedures
3. On, gone, not locked – Walking away from the computer, leaving it unlocked or not turned off
4. Gee, what's in this attachment – Unknown email attachments can cripple by carrying viruses- put it in the trash or report it as spam
5. Weak passwords – Passwords based on information easily accessible to others
6. Loose lips – Talking in public about things you shouldn't
7. Laptops with legs – Laptops left unsecured and unattended are vulnerable to theft
8. The threat within – Statistically, most security breaches originate inside the organization

NEVER SHARE YOUR USER ID or PASSWORD WITH ANYONE

The Rules for Secure Password Management:

- You will be required to change your password every 6 months
- NEVER tell or share your password with anyone
- Create a password that's hard to guess
- If you think someone has learned your password, change it immediately

SELECT a SECURE and STRONG PASSWORD

What is a STRONG password?

A strong password has a *minimum* of eight characters and should contain *at least one of each* of the following characters:

- Uppercase letters (A-Z)
- Lowercase letters (a-z)
- Numbers (0-9)
- Punctuation marks or symbols such as: !@#$%^&*()_+=-

How to create a strong and secure password:

1. **Create a password from a sentence you can remember, like "My son John is two years old today"**

   Use first letters to form the password: msjityot

2. **Add complexity with upper case letters and numbers (and special characters)**

   MsJi2Y0t

   M$JI2y@t

3. **Don't use your work password on Internet**

   Website security could be compromised

   Keystroke logging devices may be on public computers

HIPAA Security Requirements for Access to Buildings:

- Do not share access cards, keys, or codes to enter the facility
- Immediately report lost or stolen cards, or metal keys or keypad-cipher lock combinations
- Do not allow other people to enter the facility by letting them walk behind you (tailgate) without using their own card key

HIPAA Security Requirements for Workstation Protection:

Properly safeguarding each workplace computer is one of the most important ways to protect your program's data from corruption or loss:

- **Log off** when you are done working on your computer.
- **Lock your computer** session when it is left unattended (See below for instructions)
- **Protect ePHI from unauthorized access** if you work from home or other non-office work sites on a County assignment

HOW TO LOCK YOUR COMPUTER SESSION:

1. Lock your computer session when leaving your computer unattended by holding down the Ctrl + Alt + Delete keys on your computer
2. Using your mouse, click "LOCK COMPUTER"

   –or--

   Simply press the Windows and L keys to lock your computer
3. To unlock your computer session hold down the Ctrl + Alt + Delete keys on your computer
4. Type in your password and press enter

Locking your computer session when you leave your computer unattended does not shut down any document or program you have been working on. It is a key to good security and should always be practiced – locking your computer session prevents unauthorized use.

ALWAYS REPORT ANYTHING UNUSUAL:

NOTIFY YOUR SUPERVISOR IF YOU SUSPECT A SECURITY INCIDENT

Examples of potential security incidents:

- Suspected or actual unauthorized viewing of PHI or ePHI—including fax , email or hard copy document sent to incorrect recipient
- Email sent to the wrong recipient, or unencrypted email sent outside the County network
- A virus, worm, or other malicious attack (for example, through an email attachment)
- Network, system, or facility intrusion (for example, through an outside computer hacker)
- Unauthorized access to ePHI (for example, from someone using an unlocked computer workstation left unattended)
- ePHI data loss due to disaster, failure, error, malicious changes or theft
- Any unauthorized alteration or corruption of PHI or EPHI
- Loss of electronic media (e.g., lost laptop, USB drive, smartphone, CD or tablet) that contains PHI
- An unauthorized person in a covered component facility (for example, a non-employee enters the facility behind another employee.)

IF YOU SUSPECT YOUR WORKSTATION HAS A VIRUS OR IF YOU DETECT A VIRUS,

IMMEDIATELY CONTACT THE SERVICE DESK AT 874-5555

Computer Security Key Points:

- Store all data on network servers
- Never share a log-on ID or password

- Lock your computer session when left unattended
- Report any suspected security violation
- Lock ePHI at remote sites
- Know who to contact for your questions

How is HIPAA Enforced?

The Federal Department of Health and Human Services has assigned enforcement activities to the Office for Civil Rights (OCR). Any person or organization who believes a covered entity is not complying with HIPAA requirements may file a complaint with either the covered entity and/or the OCR. Complaints can be accepted only for possible violations occurring after compliance date of April 14, 2003.

What are the Consequences of Violating HIPAA?

Covered health care components are required to develop a system of sanctions (discipline) for employees who violate the health care component's privacy policies. These sanctions are not applicable to: whistleblowers (a member of the workforce who discloses information about a covered health care component); a member of the workforce who is a crime victim; or a workforce member filing a complaint with the Office for Civil Rights (OCR), testifying, assisting or participating in an investigation, compliance review or similar proceeding.

There are both civil and criminal penalties that may be imposed by the OCR if their investigation determines a violation has taken place. Penalties for failure to comply with HIPAA are severe:

Violation Category	**Each Violation**	**Total Civil Monetary Penalty for Violations of an Identical Provision in a Calendar Year**
Person did not know (and by exercising reasonable diligence would not have known) that the person violated HIPAA	$100 - $50,000	$1.5 million
Violation due to reasonable cause but not willful neglect	$1,000 - $50,000	$1.5 million
Violation due to willful neglect but violation is corrected within the required time period (30 days)	$10,000 - $50,000	$1.5 million
Violation is due to willful neglect and is not corrected	At least $50,000	$1.5 million

- Civil - $100 fine per person per violation, $25,000 fine per year for multiple violations, $25,000 fine cap per year per requirement
- Criminal: $50,000 and/or one year prison time for knowingly or wrongfully disclosing or receiving PHI protected by HIPAA; committing the offense under false pretenses, $100,000 fine and/or five years prison time; intent to sell PHI protected by HIPAA or client lists for personal gain or malicious harm, $250,000 fine and/or 10 years prison time.

Covered health care components may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against clients for exercising their privacy rights, including filing complaints.

- Any negligent or intentional violation of the HIPAA Policies and Procedures may result in such corrective action as deemed appropriate by the County.
- Any unauthorized willful or malicious release of any information associated with Protected Health Information may result in personal civil or criminal liability.
- Violations may result in notification to law enforcement officials and regulatory, accreditation and licensure organizations.

YOU ARE RESPONSIBLE FOR PROTECTING THE CONFIDENTIAL INFORMATION OF THE COUNTY'S CLIENTS

For more information, please contact:

County of Sacramento Office of Compliance, 799 G Street, Room 217, Sacramento, CA 95814

Phone: 916-874-2999 Fax: 874-1150 Intranet: http://inside.compliance.saccounty.net