



SAN LUIS OBISPO COUNTY HEALTH AGENCY

Jeff Hamm, Health Agency Director

Confidentiality and Privacy in the Health Agency

As a contractor of the San Luis Obispo County Health Agency (SLOHA), you are entrusted to protect the information with which you work or to which you are exposed. In your job, you may come into contact with client health information, other personal information about clients, financial information, employee and payroll information, and information considered confidential at the Health Agency. It is critically important that you protect any confidential information that should not be disclosed. In addition to not disclosing confidential information, you must also take reasonable steps to ensure that the confidential information that you receive, regardless of its format, is protected from theft or inadvertent access. It's not only the law and our policy; it is a condition of the contractual agreement with your employer. Our collective effort to ensure the privacy and security of confidential information, upholds the County's core values, demonstrates respect for our clients, and supports compliance with state and federal laws. **NOTE: While this document will focus primarily on Protected Health Information, the principles will apply to all confidential information that you work with at the Health Agency.**

Brief Overview of Health Information Privacy and Security regulations

The Health Insurance Portability and Accountability Act of 1996, otherwise known as HIPAA, was created by the federal government to promote improvements and efficiencies in the provision of health care. A major goal of HIPAA was to protect the privacy and security of health information. HIPAA regulations include the following parts:

- **Privacy.** The privacy regulations govern who has access to Protected Health Information (PHI). They ensure that PHI is used appropriately by creating a national minimum standard of privacy (state laws can be more stringent). The privacy regulations also give clients specific rights regarding their own health information.
- **Security.** The security regulations govern how health information is protected. They establish safeguards for Protected Health Information.

While we regularly refer to HIPAA regulations, other state and federal regulations govern the privacy and security of Health Information and other personal information. Among those that most closely affect the Health Agency are 42CFR Part 2 (governing Drug and Alcohol client information), Welfare and Institutions Code Sections 5328-5830 (governing Mental Health client information) and California SB1386 (Governing Personally Identifiable Information).

Concept: Protected Health Information – Personally Identifiable Information

Protected Health Information (PHI) is information related to a person's health care treatment and/or to the corresponding payment for those services. PHI includes information that could reasonably identify an individual (client identifiers) and is connected to their sensitive health information. PHI in electronic, paper, or oral forms must be protected. Every member of the work force, even those who don't deal directly with client information, should have an understanding of what PHI is and the ways in which it must be protected. Personally Identifiable Information (PII) is similar to PHI and must also be protected. PII differs from PHI in that it does not combine personal with health information.

Client Identifiers: Names, street address, city, county, full zip code (with some qualifications), dates directly related to an individual (e.g. birth date, dates of service), telephone and fax numbers, email addresses, Social Security numbers, credit card numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate/license numbers, vehicle identifiers, internet protocol (IP) addresses, biometric identifiers (e.g. finger and voice prints), full-face images, and any other unique identifying number, characteristic, or code.

Examples of Sensitive Health Information: Diagnoses, Procedures, Medications, Physician name and specialty, Location of service (e.g. cancer center), Service type (e.g. physician office, radiology, inpatient admission), Test results, Amount charged and paid.

Concept: Use of PHI

Employees throughout the Health Agency use PHI daily to provide critical healthcare services to our Clients. Generally, PHI can be used and shared by a client's direct treatment team to provide healthcare services and for other operational purposes such as billing. When used properly, PHI supports positive outcomes in the healthcare services we provide. The permitted uses of PHI differ slightly depending on the type of healthcare being used or reviewed. Your supervisor and/or the terms of the contract will specify the appropriate uses for different types of confidential information.

Concept: Minimum Necessary

The law requires that organizations take reasonable steps to allow access only to the minimum PHI necessary to perform a specific task or job. This minimum necessary standard applies to both internal uses as well as external disclosures. Contractors and external providers must only request and receive information tailored to the specific task or job. It is important that you do not access, use or disclose more confidential information than you are authorized to access and that you need to complete your job. The minimum necessary standard is not intended to impede client care and therefore does not apply to qualified professionals involved in the direct care and treatment of the client.

Concept: Breach of PHI

Generally, there are permitted uses/disclosures of PHI and unpermitted uses/disclosures of PHI. A breach occurs when you use or disclose PHI in a manner that is not permitted by policy or law. A breach can be deliberate or accidental. Our goal as an Agency and our commitment as individuals is not to commit a breach of confidential information. While our goal is to have no breaches, we understand that there may be times when a mistake is made and you access, use or disclose PHI or other confidential information improperly. When this happens, it is our policy and the law that you immediately tell your supervisor or your County contact that you may have caused a breach.

NOTE: The best way to prevent a breach is to ask a supervisor or County contact person PRIOR to access, use or disclosure if you are unsure about whether you are authorized and/or whether you are using the correct procedures/safeguards.

Concept: Disclosure of PHI

While you may access and use PHI as part of your job, you may also be asked to disclose PHI to others for a variety of reasons. There are a few permitted reasons that you may disclose PHI to others without a client's written approval (Authorization). Reasons include discussing a client's own healthcare information with them or providing a copy of the information to the client. The Health Agency may also use PHI without a client's authorization for the purposes of treatment, payment, or healthcare operations. The rules for disclosing PHI vary by division and you should familiarize yourself with policy and regulations prior to disclosing any PHI. In addition, always ask your supervisor for guidance if you are unsure about permitted reasons for disclosure.

Concept: Authorization

Generally, PHI may be used by the Health Agency for treatment, payment, or healthcare operations. A written authorization from the client is required for many uses and disclosures that fall outside of treatment, payment, and operations. The Health Agency has a form that the client may use, but occasionally another healthcare provider will present an authorization from the client requesting our records. It is important that no PHI be disclosed unless the authorization form is determined to be authentic and complete. Once an authorization is signed, a client has the right to revoke or cancel it at any time. HIPAA specifically states that care cannot be conditional upon a client's signing of an Authorization. Until you are trained on the Health Agency's policies and procedures regarding the disclosure of PHI or other confidential information, you should request assistance from a supervisor.

Privacy and Security Policies and Procedures

Be familiar with HIPAA Privacy and Security Policies and Procedures. Privacy Policies can be found on the Health Agency Intranet Site by clicking on "Policies & Procedures." Your supervisor and/or contract may also specify special policies related to your use and access of PHI.

Concept: Safeguards

The law requires the Health Agency to implement and maintain appropriate safeguards to protect PHI from unauthorized access, use and disclosure. Safeguards you must use and support include:

- Never access or look at a client record that you do not have permission and a business need to see. Access to electronic client records is logged by the system and monitored by our Information Technology Team. Unauthorized access is reported.
- Never discuss a client (even the existence of a client) with anyone outside of the authorized treatment or operations team. (This can be one of the most common and damaging forms of breach). If unsure who you may discuss a client with, ask for guidance from a supervisor.
- Always create strong passwords for system access and never share any of your passwords with anyone. Do not ask others to use their passwords.
- Always lock your computer using (Window key+L) when you leave it unattended for even a minute. Ensure that no one can watch you logon, and ensure that those who are not authorized cannot see your computer screen when you are viewing confidential information.
- Ensure your computer automatically locks, requiring a password to unlock, after no more than ten (10) minutes of inactivity. Our IT team can help you set this up. (Call x2800)
- Safeguard the placement of computers, printers, and fax machines to limit potential access by unauthorized users. Retrieve documents from printers and fax machines right away.
- Any computer accessing or storing PHI must be encrypted to prevent access in case of loss or theft.
- You may not access or store PHI via any mobile device (cell phone, laptop, tablet, kindle, flash drive, etc.) For example, you must never download PHI on a compact disk or an unencrypted flash drive.
- You must ensure that all confidential information in paper form is always in your direct control or is locked in a secure location where it can be accessed only by authorized users. Dispose of confidential paper through shredding or by placing the item in *locked*, confidential recycling bins.
- Secure all client credit information. Do not leave receipts or files containing client information including credit card numbers in an unsecured manner. If you must temporarily write down a client credit card number or social security number, be sure to shred the paperwork after you are finished using it.
- All electronic communication containing County information must include a confidentiality statement.
- All PHI sent via e-mail outside of the County e-mail system must be encrypted. Never include confidential information in the subject line of an e-mail. When sending an e-mail containing PHI or PII internally within the Health Agency, remove information that can identify the individual (de-identify) prior to sending.
- You must ensure that any PHI transmitted electronically, (fax, e-mail, voicemail) is appropriately protected pursuant to SLOHA policy and you must double check that the fax number, phone number, or e-mail ID is correct. (This is one of the most common reasons for breach). Call ahead to verify the fax number or e-mail and let the person to whom you are sending the information know when to expect the PHI.
- You must be aware of your surroundings when having verbal conversations about confidential information. Do not have conversations in hallways, break rooms, cubicles, or other places where others may be able to hear. Unpermitted disclosure through someone overhearing a conversation is still a breach.
- If you overhear a confidential conversation in a public hallway or elevator, ask the individuals to move to a private location to continue the discussion.

Questions about privacy and security of information at the Health Agency may be directed to:

Compliance and Privacy Officer for the Health Agency is:

Ken Tasseff - (805) 781-4788

e-mail – katasseff@co.slo.ca.us



SAN LUIS OBISPO COUNTY HEALTH AGENCY

Jeff Hamm, Health Agency Director

CONFIDENTIALITY STATEMENT

It is the responsibility of all San Luis Obispo County Health Agency (SLOHA) employees, contractors and volunteers to use, protect, and preserve personal and confidential client, employee, financial, or strategic business information in accordance with state/federal laws and County policy.

I understand that, in the course of my work, I may learn information which is confidential under federal and state law, or which is considered confidential and/or proprietary by SLOHA. Examples include but are not limited to client health information, other information considered personal by clients and their families, financial information, and employee and payroll information. I agree to keep confidential all such information, whether verbal, written or computerized, which I learn in the course of my work at SLOHA. I will not discuss client or family information with anyone not immediately involved with a client's care, treatment or operations without that client's authorization. I will not discuss client or other confidential information with anyone who does not have an authorized need to know. In addition, I will not discuss confidential or proprietary information in areas where others may overhear such discussions (such as hallways, cubicles, elevators, etc.).

I will not access or attempt to access any information unless the information is relevant to my job and I am authorized to access it. I understand that the logon ID, computer password and electronic signature assigned to me by SLOHA are to be used solely by me for my authorized access to information. I understand that use of my ID and password by anyone other than me is strictly prohibited. I will not share my password with anyone and I will take all necessary steps to protect the confidentiality of my login information. I also understand and agree that the use of my ID and password to use SLO County electronic systems constitutes a digital signature and is the equivalent of my handwritten signature on the documents.

I understand that all SLOHA software and hardware including the County e-mail system and electronic health records system are County property and subject to monitoring and review. I agree that I will only use computing devices, such as desktop computers, laptop computers, tablets, mobile phones and external storage that are protected by approved SLOHA encryption software before using them for any purposes involving protected health information and/or confidential information. I will secure my computer by locking my terminal (Windows key + L) prior to leaving it unattended and I will lock confidential documents or devices in a secure location prior to leaving them unattended. I understand that I may be personally responsible for any breach of confidentiality resulting from an unauthorized access to data on that device due to theft, loss or any other compromise. I will contact the IT Service Desk at (805) 781-2800 for questions about encryption or other software or hardware security.

I have received a copy of the Health Agency guidance entitled, "Confidentiality and Privacy in the Health Agency." I understand that any violation of SLOHA or County policies and procedures may result in termination of contract and/or disciplinary action against me including termination of employment. Further, violation of State and federal laws also provide for civil action under the provisions of Welfare and Institutions Code Section 5330, for the greater of the following amount:

- 1.) Ten thousand Dollars (\$10,000)
- 2.) Three times the amount of actual damages, if any sustained by the plaintiff.

This agreement shall remain in effect during my relationship with SLOHA and shall continue thereafter. I agree that upon completion of contract, separation, termination or if for any other reason I am not affiliated with SLOHA, I will continue to abide by the confidentiality provisions in this agreement. I further agree that upon completion of contract or upon leaving SLOHA, I will not remove any confidential or proprietary information from the County and I will return any and all confidential and/or proprietary information I may have in my possession.

I have read the above confidentiality statement and I agree to comply fully with its terms.

Signature

_____/_____/_____
Date



SAN LUIS OBISPO COUNTY HEALTH AGENCY

Jeff Hamm, Health Agency Director

CONFIDENTIALITY STATEMENT

It is the responsibility of all San Luis Obispo County Health Agency (SLOHA) employees, contractors and volunteers to use, protect, and preserve personal and confidential client, employee, financial, or strategic business information in accordance with state/federal laws and County policy.

I understand that, in the course of my work, I may learn information which is confidential under federal and state law, or which is considered confidential and/or proprietary by SLOHA. Examples include but are not limited to client health information, other information considered personal by clients and their families, financial information, and employee and payroll information. I agree to keep confidential all such information, whether verbal, written or computerized, which I learn in the course of my work at SLOHA. I will not discuss client or family information with anyone not immediately involved with a client's care, treatment or operations without that client's authorization. I will not discuss client or other confidential information with anyone who does not have an authorized need to know. In addition, I will not discuss confidential or proprietary information in areas where others may overhear such discussions (such as hallways, cubicles, elevators, etc.).

I will not access or attempt to access any information unless the information is relevant to my job and I am authorized to access it. I understand that the logon ID, computer password and electronic signature assigned to me by SLOHA are to be used solely by me for my authorized access to information. I understand that use of my ID and password by anyone other than me is strictly prohibited. I will not share my password with anyone and I will take all necessary steps to protect the confidentiality of my login information. I also understand and agree that the use of my ID and password to use SLO County electronic systems constitutes a digital signature and is the equivalent of my handwritten signature on the documents.

I understand that all SLOHA software and hardware including the County e-mail system and electronic health records system are County property and subject to monitoring and review. I agree that I will only use computing devices, such as desktop computers, laptop computers, tablets, mobile phones and external storage that are protected by approved SLOHA encryption software before using them for any purposes involving protected health information and/or confidential information. I will secure my computer by locking my terminal (Windows key + L) prior to leaving it unattended and I will lock confidential documents or devices in a secure location prior to leaving them unattended. I understand that I may be personally responsible for any breach of confidentiality resulting from an unauthorized access to data on that device due to theft, loss or any other compromise. I will contact the IT Service Desk at (805) 781-2800 for questions about encryption or other software or hardware security.

I have received a copy of the Health Agency guidance entitled, "Confidentiality and Privacy in the Health Agency." I understand that any violation of SLOHA or County policies and procedures may result in termination of contract and/or disciplinary action against me including termination of employment. Further, violation of State and federal laws also provide for civil action under the provisions of Welfare and Institutions Code Section 5330, for the greater of the following amount:

- 1.) Ten thousand Dollars (\$10,000)
- 2.) Three times the amount of actual damages, if any sustained by the plaintiff.

This agreement shall remain in effect during my relationship with SLOHA and shall continue thereafter. I agree that upon completion of contract, separation, termination or if for any other reason I am not affiliated with SLOHA, I will continue to abide by the confidentiality provisions in this agreement. I further agree that upon completion of contract or upon leaving SLOHA, I will not remove any confidential or proprietary information from the County and I will return any and all confidential and/or proprietary information I may have in my possession.

I have read the above confidentiality statement and I agree to comply fully with its terms.

Signature

_____/_____/_____
Date