Health Information Privacy and Security Policy and Procedure Suite

TABLE OF CONTENTS

San Luis Obispo County Health Agency

Health Information Privacy and Security Policy and Procedure Suite

Chapter 1
Privacy Policies & Procedures

General Privacy of Protected Health Information and Personally Identifiable Information

I. PURPOSE

These policies and procedures are intended to ensure compliance with statutes, regulations and contractual obligations that govern the privacy and confidentiality of protected health information (PHI) and personally identifiable information (PII) created, maintained, accessed and stored by the San Luis Obispo County Health Agency (SLOHA).

This policy and procedure addresses the general privacy of protected health information and personally identifiable information.

II. SCOPE

This policy and procedure document applies to all individuals who may access, use, or disclose SLOHA protected health information and/or personally identifiable information.

III. AUTHORITY

The Health Agency Director is responsible for enforcing policies, procedures and standards that provide adequate privacy and security of protected health information created, maintained, accessed, and stored by the San Luis Obispo County Health Agency. Compliance with these policies and procedures is mandatory for covered components pursuant to various state and federal statutes, regulations and contractual agreements including 45 CFR 164.500-164.534 (Subpart E, Health Insurance Portability and Accountability Act (HIPAA) – Privacy of Individually Identifiable Health Information).

IV. STATEMENT OF DESIGNATION AS A HYBRID ENTITY UNDER HIPAA

As an organization, some departments within with County engage in activities that are subject to HIPAA regulations. As such, the County is a covered entity as defined by HIPAA. Because the County also has departments that do not engage in activities subject to HIPAA regulations, the County is permitted to exclude non-covered functions, thus establishing the County as a hybrid entity as defined in section 45 CFR 164.103 of the HIPAA regulations. For purposes of compliance with HIPAA regulations, the Health Agency worked with the Office of County Counsel to identify those functions subject to HIPAA regulations. County Counsel supported findings that several functions within the Health Agency are “covered components” under HIPAA. By way of this policy and procedure document, the Health Agency Director has designated the following functions within the San Luis Obispo County Health Agency to be covered components that are subject to with HIPAA regulations and these policies.

A. Covered components of the Health Agency include:

1. Behavioral Health Department
2. Public Health Department, *excluding*:
   - Environmental Health Services Division
   - Health Promotions Division (except Oral Health Program which is a covered component)

B. Non-covered components of the Health Agency include:

1. Animal Services
2. Office of the Public Guardian
3. All programs within the Health Promotions Division with the exception of the Oral Health Program

V. POLICY AND PROCEDURE

A. General

1. SLOHA will safeguard protected health information and personally identifiable information about clients who apply for or receive services.

2. To the extent permitted by law, SLOHA may collect, maintain, use, transmit, share and/or disclose confidential information about individuals to the extent needed to administer Health Agency programs, services and activities. Confidential Information collected will be safeguarded in accordance with this policy and procedure.

B. Safeguarding Confidential Information

1. SLOHA, its employees, and business associates shall respect and protect the privacy of records and protected health information about clients who request or receive services from SLOHA.

2. Employees shall protect all health information and personally identifiable information on SLOHA clients in accordance with SLOHA privacy policies and procedures, SLOHA security policies and procedures, and State/federal regulations. Paper files containing PHI shall be in employee's control at all times.

3. Employees shall not use protected health information unless authorized by the Health Agency and only to the extent necessary to do their job.

4. Employees shall not disclose protected health information unless authorized by the Health Agency and consistent with this policy and procedure.

C. Employee Confidentiality Statement

All employees of the Health Agency shall sign the SLOHA Confidentiality Statement prior to working with any PHI or PII and annually thereafter.

D. Client Access and Privacy Rights

SLOHA policies and procedures, as well as other federal and state laws and regulations, outline a client's right to access their own protected health information, with some exceptions. These policies also describe specific actions that a client can take to request restrictions or amendments to their protected health information, and the method for filing complaints. These specific actions are outlined in SLOHA's "Client Privacy and Access Rights" policy and procedure.

E. Business Associate Agreement

1. A business associate is an individual or organization that is not part of SLOHA's workforce and acts on behalf of the County. The business associate performs functions or activities involving the use or disclosure of protected health information.

2. SLOHA may disclose protected health information to a business associate and allow a business associate to create or receive PHI on its behalf, if SLOHA obtains satisfactory assurance that the business associate will safeguard the information through a written contract. (Business Associate Agreement)

3. SLOHA will take reasonable steps to cure breaches or end violations, and if unsuccessful, may terminate a contract with a non-compliant Business Associate.

F. SLOHA Notice of Privacy Practices

1. Upon first service delivery or as soon as practicable, employees shall provide a copy of the “Notice of Privacy Practices” (NPP), to all clients applying for or receiving covered services from SLOHA or enrolled in a County health plan.

2. Employees shall seek to acquire a signed acknowledgement from clients accepting the NPP and if not able to secure a signed acknowledgment, shall notate that the client refused to acknowledge receipt in the client’s record.

3. If a client refuses to accept a Notice of Privacy Practices after being offered, the employee shall notate the refusal in the client’s record.

G. Use and Disclosures for Research Purposes

1. SLOHA may use or disclose a client’s protected health information for research purposes and studies. All such research disclosures are subject to applicable requirements of state and federal laws and regulations and to the specific requirements of this policy and procedure.

2. SLOHA may use or disclose a client’s protected health information to conduct public health studies, studies that are required by law, and/or studies or analysis related to its health care operations. All such research disclosures are subject to applicable requirements of state and federal laws and regulations and to the specific requirements of this policy and procedure.

H. De-Identification of Protected Health Information / Use of Limited Data Sets [164.514]

1. De-Identified Information

a. De-Identified Health Information is health information that does not identify an individual, and to which there is no reasonable basis to believe that the information can be used to identify an individual. De-identified health information is not PHI and therefore is not protected by the Privacy Rule.

b. Unless otherwise restricted or prohibited by other federal or state law, SLOHA may use and share de-identified protected health information for business related purposes and as appropriate without further restriction.

2. Limited Data Set

a. A limited data set is described as health information that excludes certain, listed direct identifiers (see below) but that may include city; state; ZIP Code; elements of date; and other numbers, characteristics, or codes not listed as direct identifiers.

b. SLOHA may disclose a limited data set only for the purposes of research, health care operations, or public health purposes. However, SLOHA is not restricted to using a limited data set for its own activities or operations.

c. Where SLOHA and a business associate are both governmental entities, County may disclose to the business associate a limited data set to carry out a health care operations function if County has a data use agreement with the business associate.

d. SLOHA may use or disclose a limited data set that meets the requirements of State/federal regulations if SLOHA enters into a data use agreement with the limited data set recipient.

I. Complaints Regarding Application of this Privacy Policy and Procedure [164.530]

1. Clients or employees may file complaints concerning:
    a. Disagreements with SLOHA's privacy policies and procedures.
    b. Suspected violation in the use, disclosure, or disposal of the client's PHI or PII.
    c. Denial of access to PHI.
    d. Denial of amendments to PHI.
2. Complaints must be filed in writing, either on paper or electronically. (Link to Form)
3. Complaints may be filed with the SLOHA Privacy/Compliance Officer or sent to the Secretary of the Department of Health and Human Services in accordance with SLOHA Notice of Privacy Practices.
4. The complaint must describe the acts or omissions believed to be in violation and should when possible name the person believed to be involved.
5. San Luis Obispo County will not intimidate, threaten, coerce, discriminate against or take other retaliatory action against any person filing a complaint or inquiring how to file a complaint.
6. SLOHA will not require clients to waive their rights to file a complaint as a condition of providing treatment, payment, and enrollment in a health plan, or eligibility for benefits.
7. Employees shall immediately forward complaints from clients or co-workers to the Privacy/Compliance Officer for appropriate handling.

J. Conflict with Other Privacy Laws

1. SLOHA has adopted reasonable policies and procedures for the administration of its programs, services, and activities. If any state or federal law or regulation or order of a court having appropriate jurisdiction, imposes a more stringent requirement related to the privacy of confidential information, SLOHA shall act in accordance with the standard requiring stricter protection from disclosure or more permissive access to the client.
2. In the event more than one policy or procedure applies, and compliance with all such policies cannot be reasonably achieved, SLOHA employees shall seek guidance from an immediate supervisor. If an employee has additional questions regarding this policy and procedure or if a privacy/disclosure matter is complex, the employee and/or supervisor should consult with the HIPAA Privacy Officer in appropriate circumstances.

VI. APPLICABLE STANDARDS/REGULATIONS

- HIPAA 45 CFR 164.100 – 164.534
- H&S 5328 – 5328.9
- 42 CFR, Part 2
- California Civil Code 56.10 – 56.11
- H&S 123100-

Client Privacy and Access Rights

I. PURPOSE

This policy and procedure addresses clients' rights related to their protected health information including the right to access the information, request modification, and receive a Notice of Privacy Practices.

II. SCOPE

This policy and procedure document applies to all employees who may access, use, or disclose SLOHA PHI.

III. POLICY

SLOHA clients are granted the following rights based on HIPAA statutes, other state and federal regulations, and contractual agreements. For deceased clients, the client representative (next of kin or executor of estate) has the rights that the client would have had relative to access and release of the record. **Disclosures described in this Client Privacy and Access Rights policy and procedure may only be performed by a Custodian of Records**.

A. Clients have the right to receive a written notice explaining how PHI will be used and disclosed. (Notice of Privacy Practices)

B. Clients have the right to access and obtain a copy of their protected health information in a designated record set, consistent with federal and state law, with some exceptions as shown in the procedures section of this policy and procedure.

C. Clients have the right to request an amendment of their protected health information in the designated record set. Some restrictions apply as shown in the Procedures section.

D. Clients have the right to obtain an accounting of disclosures of their PHI (with limited exceptions).

E. Clients have the right to request that certain information be restricted from use or disclosure for purposes of treatment, payment or health care operations (although regulations allow SLOHA to use its discretion in agreeing to such requests).

F. Clients have the right to request restrictions on the manner and method of confidential communications.

G. Clients have the right to submit a complaint if they believe their PHI has been used or disclosed improperly.

H. Clients have the right to be notified in the case of breach of their PHI. Disclosures related to a breach of PHI may only be performed by a HIPAA Privacy Officer.

IV. PROCEDURE

A. Right to Receive a Notice of Privacy Practices (NPP) [164.520]

1. Upon first service delivery or as soon as practicable, employees shall provide a copy of the "Notice of Privacy Practices" (NPP), to all clients applying for or receiving covered services from SLOHA. Clients may receive additional copies of the NPP upon request.

   Individuals detained in the County Jail or the County Juvenile Detention Facility do not have the right to receive the NPP.

2. Employees shall seek to acquire a signed acknowledgement from clients accepting the NPP.
    a. If the client agrees to sign an acknowledgement, the employee shall have the client sign the NPP Acknowledgment form and shall file the signed form in the client record. Alternatively, if receipt acknowledgement is on a combined log sheet, the client may sign the log and the log shall be retained for a minimum of six years.
    b. If the client accepts the NPP but is unwilling to sign the NPP Acknowledgement form or if the client refuses to accept the NPP, the employee shall notate the refusal on the NPP Acknowledgement Form and shall file the notated form in the client record.
3. A copy of the notice shall be posted in clear and prominent locations where it is reasonable to expect clients to be able to read it. Additionally, the notice will be posted and available electronically on the SLOHA web site.
4. SLOHA reserves the rights to revise its Notice of Privacy Practices at any time to comply with state/federal regulations or operational needs.

B. Right to Access PHI [164.524]
1. Upon request, (with some exceptions) SLOHA will allow a client to inspect and/or obtain a copy of their medical information that is used to make decisions about their care. This may include medical and billing information, but may not include some mental health information not entitled by regulation.
2. Employees may discuss the request for medical information with a client, but only to seek clarity about the exact information or documents that the client seeks. Employees may not discourage a client from requesting their medical information.
3. Access to medical information shall be limited to the Designated Record Set as defined in 45CFR 164.501.
4. Employees shall make reasonable efforts to verify identity of the requesting client prior to disclosing information.
5. Pursuant to Health & Safety Code 123110, granted requests for access shall be provided within the following timeframes:
    a. Requests to inspect patient records by the patient or personal representative shall be granted within 5 working days of the request.
    b. Requests for copies of patient records by the patient or personal representative shall be granted within 15 working days of the request.
6. Whenever reasonable, access to or copies of requested medical information shall be provided in the form and format (paper, electronic, etc.) requested by the client.

C. Denial of Access to PHI
1. Denial of access to mental health information

    Access to mental health information can be denied if a licensed mental health care professional (physician, psychologist, LMFT, LPCC, or LCSW) has determined that the access requested may result in: (H&S Code 123115(a)-(b))
    a. (For all clients) substantial risk of significant adverse or detrimental consequences to the client; or,

b. (For minor clients) a detrimental effect on the provider's professional relationship with the minor patient or the minor's physical safety or psychological well-being.

2. Denial of access to health information by correctional inmates

a. SLOHA Law Enforcement Medical Care (LEMC) staff may deny an inmate's request to access, in whole or in part, the inmate's PHI if such access would jeopardize the health, safety, security, custody, or rehabilitation of the inmate or other inmates, or the safety of any officer, employee, or other person at the correctional facility or person responsible for the transport of the inmate.

b. If an inmate requests their PHI in a form or format that is inconsistent with custody safety and security rules, such as a large amount of paper or an electronic storage device, LEMC staff shall offer an alternative, such as a written summary explanation of the information or other reasonable alternatives.

3. Procedure for denial of access to medical information

a. If access to medical information is denied, the client will be notified of the reason for denial including whether the denial is subject to review pursuant to 45CFR 164.524(d). The person denying the amendment shall review and comply with section 164.524(d) to ensure that all statutory procedures are followed. If the denial is subject to review, the notification shall include instructions for how to appeal and procedures for the review process.

b. If access to medical information is denied, the client may authorize their own mental health professional to review their health records pursuant to Health & Safety Code 123115(b)(2).

D. Fees

1. SLOHA may charge a reasonable, cost-based fee for providing copies of PHI, including the cost of an electronic storage device, copying (supplies and labor), postage, and preparation of any summary or explanation. Charges shall be based on the SLOHA cost schedule, but in no case shall exceed maximum charges specified in Health & Safety Code 123110(b).

2. Copying Cost Schedule:

a. Client Fees: Copying: $0.10 per page + Postage

b. Attorney Fees: Copying: $0.10 per page + Postage

c. Social Security or Vocational Rehabilitation:

Copies: The enumeration for copying pertinent medical record is:
1 to 20 pages $14.05
21 to 25 pages $15.40
26 to 30 pages $16.75
31 to 35 pages $18.10
36 to 40 pages $19.45
41 to 45 pages $20.80
46+ pages $21.60

Postage: No fees as they provide prepaid postage and prefer faxes

Preparation of Summary:
0-60 minutes $30.00 for a narrative report summary by professional staff.
60+ minutes $50.00

d. Summary Alternative Fees: $13.00 per quarter hour + Postage.

E. Right to Request an Amendment to PHI [164.526]

1. SLOHA shall provide clients with the right to request an amendment to their PHI for as long as such PHI is maintained by the SLOHA.
2. Requests for amendments must be submitted in writing on a Request to Amend Health Record form and provide a reason that supports the request.
3. Amendments may be denied with approval of a Division Manager or higher under the following circumstances:
    a. The information being requested for amendment is accurate and complete;
    b. The PHI was not created by SLOHA;
    c. The information at issue is not part of the medical information kept by SLOHA;
    d. The information is not part of the PHI that the client would be permitted to access and obtain a copy; or
    e. SLOHA may not amend the information pursuant to state/federal regulations.
4. If a request to amend PHI is denied, the person denying the amendment shall review and comply with section 164.526 of the HIPAA regulations to ensure that all statutory procedures are followed. Such requirements include notification to the client of the reason for denying the request. The notification shall contain:
    a. The basis for the denial
    b. A statement that the client may provide a statement of disagreement to be included in the medical record
    c. That the client may request that SLOHA include a copy of the denial and the statement of disagreement in any future disclosures
    d. Instructions on how the client may complain to SLOHA [164.530] and instructions on how the client may complain to the Secretary of HHS [160.306].
5. If a request to amend PHI is denied, the client shall have the right to submit a written addendum, with respect to any item or statement that the client believes is incomplete or incorrect. SLOHA may include a rebuttal to the written addendum
6. The denial letter, client's addendum and SLOHA rebuttal shall be attached to his/her records and included whenever SLOHA makes a disclosure of the item or the statement that the client believes to be incomplete or incorrect.

F. Right to an Accounting of Disclosures [164.528, W&I Code 5328.6]

1. SLOHA shall respond in writing to any client requests for an accounting of how their PHI has been disclosed. Such response and accounting shall include:
    a. A list of disclosures for the six years prior to the request, unless the client wants information for a shorter time period;
    b. Disclosures made to or by business associates;
    c. The date of each disclosure;
    d. The name of the person or entity who received the PHI, including an address if possible;
    e. A brief description of the information disclosed; and
    f. A brief statement of the purpose of the disclosure.

2. Accountings do not need to include disclosures made for the following purposes:
    a. For treatment, payment or health care operations within the Health Agency;
    b. To clients regarding their own information;
    c. Pursuant to an authorization signed by the client or their authorized representative;
    d. For use in the facility's directory;
    e. To persons involved in the client's care;
    f. For notification purposes (e.g. to notify a family member, personal representative or other person of the client's location, general condition or death);
    g. For national security or intelligence purposes;
    h. To correctional facilities or law enforcement officials; or
    i. For any other disclosure allowed by State/federal law that does not require accounting to the client.
3. Clients will be provided the first accounting of disclosures free of charge. A reasonable, cost-based fee may be charged for each subsequent request for an accounting within the same 12-month period as long as the client has been informed in advance of the fee and the client has had the opportunity to withdraw or modify the request.

G. Right to Request Restrictions on PHI [164.522]

1. The SLOHA Privacy Officer, Compliance Officer, or Compliance Program Manager shall consider a client's request that we restrict our use or disclosure of their PHI for treatment, payment or healthcare operations purposes; that is, a client may request that SLOHA voluntarily agree not to use or disclose PHI in a way that the law would otherwise allow. SLOHA shall also consider a client's request to restrict information that may be released to family or friends.
2. Requests for restrictions must be made in writing and include the following:
    a. What information to limit;
    b. Whether the limitation is for use, disclosure, or both; and
    c. To whom the limitation applies (e.g. disclosure to a spouse).
3. Although clients shall be given the right to make such requests, SLOHA is not required to agree to the request except if the request is to restrict:
    a. Information about service or treatment for which the individual or person, other than the health plan or entity, paid for in full.
    b. The disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law.
4. Upon agreement to a restriction, the agreement can only be broken during a medical emergency and only if the restricted information is needed to provide the emergency treatment.

5. An agreement to restrict information doesn't prevent uses or disclosures made for the following purposes and consistent with HIPAA, W&I Code 5328, and 42CFR Part 2:
    a. For public health activities;
    b. For reporting abuse, neglect, domestic violence or other crimes;
    c. For health agency oversight activities or law enforcement investigations;
    d. For judicial or administrative proceedings;
    e. For identifying decedents to coroners and medical examiners or determining a cause of death;
    f. For uses or disclosures otherwise required by law.
6. An agreement to a special restriction may be terminated as follows:
    a. The client agrees to or requests the termination in writing;
    b. The client orally agrees to the termination and the oral agreement is documented; or
    c. The provider informs the client that it is terminating the agreement; however, the termination shall be effective only with respect to PHI created or received after the client has been notified of the termination.
7. A provider that agrees to a special restriction must document the restriction. Such documentation must be retained for at least six years.

H. Right to Request Confidential Communication through Alternate Means or Location. [164.522]
1. For clients receiving treatment, SLOHA will consider a client's request to receive communications of PHI by alternative means or at alternative locations. For example, some clients may not want their appointment notices, bills, or explanation of benefits to go to their home where family members may see it.
2. For clients in health plans, SHOHA *must* comply with a client's request to receive communications of PHI by alternative means or at alternative location if the client states that the disclosure could endanger the client.
3. SLOHA will accommodate reasonable requests and shall not require an explanation from the client as to why he/she is requesting an alternative means or location of communication.

I. Right to Submit a Complaint if a Client Believes PHI has been Improperly Used or Disclosed.
1. Clients may submit a complaint to the HIPAA Privacy Officer, Security Officer, Compliance Officer, or Compliance Program Manager if they believe their PHI has been improperly used or disclosed. The complaint may be submitted orally, but may also be submitted on a PHI Privacy Complaint Form.
2. SLOHA employees shall assist any client who reasonably needs assistance filling out a complaint form.
3. The HIPAA Privacy Officer shall log all complaints regarding improper use or disclosure of PHI and shall maintain the information for no less than six years.

J. The Right to be Notified in the Case of Breach of Their Unsecured PHI. [164.404]

1. The SLOHA Privacy Officer, Compliance Officer, or Compliance Program Manager shall notify any client whose unsecured protected health information has been or is reasonably believed to have been accessed, acquired, used or disclosed as a result of a reportable breach.

2. The Privacy Officer, Compliance Officer, or Compliance Program Manager shall have responsibility for notifying clients of a breach. No other employee shall contact a client regarding a breach without permission of the Health Agency Director.

V. APPLICABLE STANDARDS/REGULATIONS

- HIPAA 45 CFR 164.100 – 164.534
- H&S 5328 – 5328.9
- 42 CFR, Part 2
- California Civil Code 56.10 – 56.11
- H&S 123100-

Use and Disclosure of Protected Health Information

I. Purpose

These policies and procedures are intended to ensure compliance with statutes, regulations and contractual obligations that govern the privacy and confidentiality of health information created, maintained, accessed and stored by the San Luis Obispo County Health Agency (SLOHA)

This policy and procedure addresses the appropriate use and disclosure of client's protected health information.

II. SCOPE

This policy and procedure document applies to all individuals who may access, use, or disclose SLOHA PHI.

III. POLICY AND PROCEDURE

A. General Policy

SLOHA shall not use, or disclose PHI without a written authorization signed by the individual, or by the individual's personal representative, unless the disclosure or use without written authorization is permitted or required by law. When SLOHA receives or obtains a valid authorization, the use or disclosure of PHI must be consistent with such authorization.

B. Minimum Necessary Use, Request or Disclosure [45CFR 164.502 & 164.514]

1. PHI and PII shall only be accessed, used, requested and/or disclosed for job related purposes. It is a violation of this policy and procedure to access any protected medical information unless done so in the scope and course of the job.
2. When using, requesting or disclosing PHI or PII, employees shall make reasonable efforts to limit the use or disclosure to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.
3. Exceptions
    a. Disclosures to the client or client representative pursuant to client access rights;
    b. Uses or disclosures made pursuant to a valid HIPAA authorization which describes the PHI to be disclosed;
    c. Disclosures made to the Secretary of the United States Department of Health and Human Services pursuant to an investigation or compliance review; and
    d. Other uses or disclosures that are required by law and that commonly prescribe what information must be disclosed (e.g., pursuant to a subpoena or court order, reporting child abuse, or any other use or disclosure of PHI that is required by law).

C. Mandatory Disclosures [45CFR 164.524 or 164.528]

SLOHA is statutorily mandated to disclose PHI in the following circumstances:

1. To an individual or authorized personal representative regarding their own information, when requested under certain rights to access, inspect, and copy their PHI and to obtain an accounting of disclosure.
2. To the Secretary of U.S. Department of Health and Human Services to investigate a complaint or to determine compliance with HIPAA regulations.

3. SLOHA employees must disclose PHI without an individual's authorization if required by law [45CFR 164.512(a)], and the disclosure complies with, and is limited to, the relevant requirements of such law. Such disclosures include:

    a. Drug and Alcohol Treatment Programs: Reporting of child abuse and neglect

    b. Mental Health Treatment Programs: Reporting of child abuse and neglect, reporting of elder abuse and neglect, and reporting when a client is a serious threat of violence (Tarasoff Warning).

    c. Public Health Treatment Programs: Reporting of child abuse and neglect, reporting of elder abuse and neglect, reports of abuse and assault by another person, reports of injury by firearms.

D. Permitted Disclosures **without an Authorization** (Mental Health and Public Health)

SLOHA employees may use and disclose minimum necessary client PHI without an authorization for the following purposes:

1. Treatment, Payment and Health Care Operations
[45CFR 164.502, 164.506; W.I. Code 5328(a), 5328(c)]

    Employees involved in the treatment of the client, in payment activities or in healthcare operations, may use or disclose client PHI without written authorization, subject to the minimum necessary standard, for the following purposes:

    a. For treatment purposes between qualified professionals in the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another. Treatment purposes include:

        i. Uses, discussions and other disclosures with qualified professionals associated with the client's care

        ii. Discussions with a supervisor for purposes of treatment guidance

        iii. Discussions within treatment team meetings and with others supporting treatment of the client.

        iv. Disclosures to the Behavioral Heath Patient's Rights Advocate,

        Note: Qualified Professionals may only disclose drug and alcohol treatment information within the Drug and Alcohol treatment program.

    b. For payment purposes to obtain reimbursement to determine eligibility or coverage of health benefits or medical necessity, for utilization review, and in the case of a SLOHA health plan, to fulfill responsibilities for coverage and provision of benefits.

    c. For health care operations to perform quality assessment and improvements, fraud detection, conducting medical reviews, business planning, general administrative activities, and other activities allowed pursuant to 45CFR 164.506.

2. Response to a Client's Medical Emergency

    Employees may use or disclose PHI to the extent needed to provide emergency treatment if a client does not have the capacity to make healthcare decisions or is otherwise incapacitated.

3. Disclosures to Department of Social Services (DSS) Staff

   SLOHA staff may disclose information necessary to coordinate care, to DSS staff, without an authorization when all of the following apply:

   a. The disclosure pertains to a minor detained pursuant to Welfare & Institutions Code 300. ("Detained" means removed from parental custody or care.); **and**

   b. The court issues an order authorizing DSS to obtain and to coordinate health services; **and**

   c. The information disclosed is, in the treatment professional's clinical opinion, reasonably necessary for the coordination of the minor's care. NOTE: The court order must specify the type of treatment, (for example: mental health-related treatment or drug and alcohol related treatment,) in order to release such information (authorization to obtain and coordinate general medical care is not sufficient). Nothing in the law or this policy requires or compels staff to disclose information given in confidence by the minor or the minor's family.

4. Law Enforcement Agencies

   Employees may disclose PHI subject to the minimum necessary standard to law enforcement officers if the information is directly related to the client's commission of a crime or threat to commit a crime *on SLOHA premises or against SLOHA personnel*. Information shall be limited to circumstances of the incident and client status including name, address, and last known whereabouts.

   For other disclosures to law enforcement, only a custodian of records shall make the disclosure. Because law enforcement may request information directly from an employee involved in client care, the following guidelines shall be observed:

Guide for Disclosure to Law Enforcement		
Scenario	**Staff Response**	**Comment**
a) **Warrant for arrest:** The police officer calls or comes to the PHF and wants to know if a client is receiving services because there is a warrant for the client's arrest.	Must Not Disclose	*Unless* the officer personally lodges a warrant of arrest or an abstract of such a warrant inquiring about a client at the PHF showing that the person is wanted for a serious *felony* (Penal Code 1192.7) or a *violent* felony (Penal Code 667.5). *Only* tell the officer whether the person is currently confined in the PHF. A call to Mental Health about any other client of ours should result in a "Must Not Disclose" answer.
b) **Missing person report:** The police officer wants to know if a client is at the PHF or if you know his/her whereabouts.	---	Ask the client to sign an Authorization for the police, in order for you to disclose. If the client does not agree, you **Must Not Disclose** to the police.
c) **Assault and battery investigation (perpetrator).** The police officer is investigating an assault and battery report and the client is the accused perpetrator.	---	Tell the officer that confidentiality laws prohibits you from disclosing the names of patients. Check with client to see if they want to authorize you to give contact information to police.
d) **Restraining order (perpetrator):** The police officer needs to deliver a restraining order to the client who is the perpetrator.	---	Tell the officer that confidentiality laws prohibit you from disclosing the names of clients. Check with client to see if they want to receive a copy of the restraining order from the police officer.
e) **Subpoena to appear in court**	Custodian of Records may Disclose	Accept the subpoena. Contact your Supervisor and Medical Record Staff immediately who will contact County Legal Counsel to discuss how to proceed.
f) **Dependent Adult Abuse Report (victim):** The police officer is investigating a Dependent Adult Abuse Report and the client is the reported victim.	Custodian of Records may Disclose	You may disclose only if YOU filed the report, not if police contact you while investigating a report made by someone else in another agency. Keep disclosure minimal. Disclosure must be limited to facts that led you to know there was abuse, reasonably suspect, or words client (victim) used to tell you about the abuse.

5. Guidelines for Authority to Disclose PHI

Based on classification, the following guidelines shall be used by employees to determine limits on their authority to disclose PHI:

Guidelines for Authority to Disclose PHI	
Drug and Alcohol Services Treatment Programs	
Treatment Professional D&A Specialist I-IV M.H. Therapist I-IV Nurse Practitioner	Drug and Alcohol Treatment Professionals may make the following disclosures: 1) **Within the substance abuse treatment team**: May disclose PHI about clients to whom they are assigned with others on the same client's treatment team. 2) **With limited exceptions such as child abuse, all other disclosures require client authorization and must be performed by a Custodian of Records.**
Public Health Treatment Programs	
Treatment Professional Public Health Nurse Correctional Nurse Community Health Nurse All N.P.s and LVN's MHT with Psych Tech licensure working at jail. Phys. and Occ. Therapist Selected Program Mgr. Comm. Disease Invest. Microbiologist P.H. Nutritionist Social Worker I-IV	Public Health Treatment Professionals may make the following disclosures. 1) **To qualified professionals involved in the client's care, provision of services, or appropriate referrals:** P.H. treatment professionals may disclose PHI about clients with others on the client's treatment team. 2) **To the client, a family member, other relative, or friend WHILE CLIENT IS PRESENT:** May disclose PHI if the client is present and has given oral consent to discuss with family member or friend. 3) **Oral disclosures requiring a signed client authorization**: P.H. treatment professionals may make oral disclosures based on a valid, complete and signed client authorization. The treatment professional must log all such disclosures. **NOTE regarding disclosures by paper, e-mail, fax, text, etc. requiring client authorization: With limited exceptions such as child/elder abuse, any disclosure via paper, e-mail, fax, text, etc., requiring a client authorization *must* be performed by a Custodian of Records.**
Mental Health Treatment Programs	
Treatment Professional M.H. Therapist I-IV Mental Health Nurse Psychologist Psychiatrist	The following guidelines are established for MH Treatment Professionals regarding disclosures to qualified professionals involved in the client's treatment or referral: 1) **All disclosures within the Health Agency umbrella of care:** MH treatment professionals may disclose PHI about clients to other qualified professionals on the client's treatment team. No logging required. 2) **Oral disclosures outside the Health Agency umbrella of care** (No authorization required)**:** MH treatment professionals may orally disclose PHI to other qualified professionals who are involved in the treatment or referral of the client *and* are outside of the Health Agency umbrella of care. No logging required. **NOTE regarding disclosures outside the Health Agency umbrella of care via paper, e-mail, fax, text, etc.:** Disclosure of PHI via paper, e-mail, fax, text, etc.to qualified professionals who are involved in the treatment or referral of the client *and* are outside of the Health Agency umbrella of care should be performed by a Custodian of Records. If delay for disclosure by a Custodian of Records would impact client care, a qualified treatment professional may make the disclosure. *The Disclosure must be logged by the employee making the disclosure and must be reported to a Custodian of Records within 24 hours of the* disclosure. 3) **Oral disclosures *requiring a signed client authorization***: MH Treatment professionals may make oral disclosures based on a valid, complete and signed client authorization. The treatment professional must log all such disclosures. **NOTE regarding disclosures by paper, e-mail, fax, text, etc. *requiring client authorization*:** With limited exceptions such as child/elder abuse, any disclosure via paper, e-mail, fax, text, etc., requiring a client authorization *must* be performed by a Custodian of Records.

CONTINUED……	
Treatment Support Staff	
Treatment Support Staff M.H. Worker Aides D&A Worker Aides Public Health Aides Physical Therapy Aides Patient Services Rep. Laboratory Assistant Select Administrative Asst.	Treatment support staff may use and access minimum necessary PHI as required to carry out the duties of their job. Treatment support staff may disclose PHI about clients to others on the same client's treatment team, and only within the Health Agency umbrella of care. Note: Selected treatment and support staff may be designated as a Custodian of Records.
	D&A Worker Aides assigned to the "Drug Testing Team" In addition to disclosure allowed for other D&A Worker Aides, may disclose PHI in appropriate format to authorized drug testing labs.
Custodian of Records	
Custodian of Records Health Information Tech. D&A Services Designee Public Health Designee M.H. Compliance Officer Privacy Officers Others as designated	A Custodian of Records may disclose PHI as authorized by their supervisor. All disclosures must be for business related purposes within state and federal guidelines.
Payment and Operations Staff	
Payment and Operations Accountant Acct. Clerk/Sr. Acct. Clerk Admin. Services Officer Selected Program Mgrs. Selected Admin. Asst. Epidemiologist Quality Support Staff	Payment and Operations staff may access, use and disclose PHI about clients within the Minimum Necessary Standard for the purposes of payment or operations. May only disclose to outside entities as authorized by their supervisor.

Health Agency Umbrella of Care For the purpose of disclosure, the "Umbrella of Care" includes the Health Agency and the following other agencies whose employees are considered part of the health agency's team for treatment, payment or operations.	THMA Kinship Center County Correctional Staff (Limited Inmate Information) Designated Drug Testing Lab	Family Care Network Child Development Center Sober Schools County Courts

E. Permitted Disclosures **Requiring an Authorization**

Any disclosure of protected health information that is not a mandatory disclosure pursuant to State/federal privacy statutes or is not described in the "Permitted Disclosures without an Authorization (Mental Health and Public Health)" policy and procedure must be supported by a signed Authorization to Disclose Protected Health Information form prior to disclosure of the information. Nothing in this section shall preclude SLOHA from requiring a signed client authorization to support any disclosure not mandated by HIPAA regulations. [Per 45CFR 164.500 – 164.534 & Welfare and Institutions Code 5328 – 5330]

1. General Policy and Procedure Regarding Disclosures Requiring Client Authorization

   Permitted disclosures requiring an authorization shall only be performed by a Custodian of Records. Exception exists for Public Health and Mental Health Treatment Professionals when making verbal disclosures requiring client authorization. (See chart above)

2. Authorization Forms

   a. When SLOHA is requesting authorization from a SLOHA client, all SLOHA divisions and units shall utilize either:

      i. Behavioral Health (MH and DAS) programs

         B.H. employees MUST use an authorization form included in a SLOHA approved Electronic Health Record system such as Anasazi. The form may be filled out in the EHR system and electronically signed (preferred), filled out in the EHR and then printed for hard copy signature, or using approved paper version only, printed and completed by hand for hard copy signatures. When a hard copy signature is obtained, the form is scanned into the EHR. Regardless how the form is completed, an electronic version is completed and final approved to enable tracking functionality within the EHR.

      ii. Public Health programs

         Public Health employees must use the SLOHA Public Health Authorization to Disclose Protected Health Information form or other form approved for your program.

   b. Authorizations received from other providers for disclosure of PHI from SLOHA to the other provider, must contain all of the HIPAA-required elements. (See Attachment A – Min. requirements for valid authorization.)

      i. Inadequate authorizations shall not be honored and should be returned to the requesting provider. (We may offer the SLOHA authorization form to the other provider as an alternative.)

      ii. An authorization is not adequate or valid if:

         - The expiration date has passed or the expiration event is known by SLOHA to have occurred;
         - The authorization has not been filled out completely;
         - The authorization is known by SLOHA to have been revoked;
         - Information in the authorization is known by the SLOHA to be false;
         - The authorization is improperly combined with another document; or
         - The authorization is not in 14-point font type. [CMIA, Section 56.11]

3. Documenting Authorizations [45CFR 164.508]

   a. All authorizations for use and disclosure of SLOHA PHI must be maintained in the medical record of the individual concerned.

   b. A copy of the completed authorization form shall be offered to the client.

4. Verification Procedures [45CFR 164.514]

   Prior to making any disclosures permitted by HIPAA or other related regulations, staff shall take reasonable precautions to verify the identity of the person requesting SLOHA PHI and the authority of any such person to have access to SLOHA PHI.

   a. For requests made in person the following may be requested:

      i. A valid driver license
      ii. A current identification badge or similar proof of official status
      iii. Positive identification by the patient
      iv. Requests must include a valid, completed authorization

b. For requests made by telephone:

i. Conversations with persons that you recognize and are authorized to discuss PHI may be made on a voice recognition basis.

ii. For all others, request caller's name, title, name and location of facility, telephone number and return the call. If uncertain about caller's identity, use alternate means of communication.

iii. A valid, completed authorization must be on file prior to making the disclosure.

c. For requests made in writing or by fax:

i. Requests must be on agency letterhead if from another provider

ii. Requests must include a valid, completed authorization

iii. (If by fax) Unless the agency or individual are recognized, call the agency or individual, verify the fax number, and advise that a confidential fax transmission is coming. Call back to ensure receipt.

5. Authorization requirements for **minors**

a. General Disclosure of a Minor's PHI

A Parent or Legal Guardian must authorize uses or disclosures of a Minor's PHI, unless Minor is:

i. Emancipated (Married, Active Military Service, By Court Order); or

ii. Self-Sufficient (age 15 or older, living separate and apart from parents, managing own finances) if relative to General Medical / Dental Care; or

iii. Allowed by law to give own consent to "Sensitive Services." Criteria includes:

- Any-Age Minor: Care related to the prevention or treatment of pregnancy, sexual assault or rape,
- Minor age 12 and older: Outpatient mental health (if "at risk" criteria are met), outpatient drug and alcohol abuse treatment, infectious, contagious or communicable disease treatment, or sexually transmitted disease / HIV testing and treatment.

b. Disclosure of PHI of a Minor who is a dependent of the Courts, DSS, or a Health Care Provider

i. Disclosure to an adult (Social Worker, Probation Officer, Etc.) who has care and custody of the Minor:

If a minor is a dependent or ward of Juvenile Court, a general health care provider (Civil Code 56.103) or mental health care provider (W&I Code 5328.04) may disclose PHI to a County social worker, probation officer or other adult who has care and custody of a minor in order to coordinate health care services and treatment (e.g., information about appointments, treatment plans, follow-up care, etc.).

ii. Disclosure to Parents when Minor is a dependent of the Courts, DSS, or a Health Care Provider:

- When Parental Access to Records is Denied by Courts

  Parental access must be denied and a parent must not be permitted to authorize third party disclosure of the record when a minor is a W&I Code 300 dependent of the court and has been removed from the physical custody of the parent (e.g., “detained”).

- When Parental Access to Records is Allowed by Courts:

  Parents *may* be given access to records of a minor who is a dependent of the Juvenile Court if the following are in place:

  - The court may make a finding that parental access would not be detrimental to the minor and may issue an order permitting the parent to access to record. The court’s order permits, but does not require, staff to allow parental access to the record.
  - The parent must present a copy of the court order to a Health Information Technician (HIT), who will make the court order part of the record.
  - The “psychotherapist” determines what the parent may safely access based on 2a and 2b above.

c. Signature Requirements:

i. DSS Family Reunification (FR) and Permanent Placement (PP) services

- Detention Order authorizing DSS staff to obtain and authorize health-related services is required and must be filed in the client’s record
- Authorization to Use/Disclose PHI not required
- DSS social worker signs Consent for Treatment

ii. DSS Family Maintenance (FM) services

- Parents (and minors aged 12 or older) retain the same legal authority to consent for treatment and to access/authorize disclosure of the record that they held before dependency.
- Parents (and minors aged 12 or older) must sign the Consent for Treatment and the Authorization to Use/Disclose PHI to facilitate disclosure of PHI to DSS.

iii. DSS Voluntary Family Maintenance (FM) services

- Minors in voluntary FM services are not dependents of the court. Parents (and minors aged 12 or older) retain the same legal authority to consent for treatment and to access/authorize disclosure of the record that they held before agreeing to voluntary FM services.
- Parents (and minors aged 12 or older) must sign the Consent for Treatment and the Authorization to Use/Disclose PHI to facilitate disclosure of PHI to DSS.

iv. Supportive Transition (ST) services to Non-Minor Dependents

- ST are transitional services for youth, aged 18 – 21, who are dependents of the court, but reached age of majority while in placement.
- Non-minor dependents have adult legal decision-making authority.
- The non-minor dependent must sign the Consent for Treatment (if not previously signed) and the Authorization to Use/Disclose PHI to facilitate disclosure of PHI to DSS.

F. Special Provisions for Disclosure of PHI in the **Public Health Division**

1. Disclosures requiring the opportunity for a client to agree or object. [45CFR 164.510]

   A Public Health employee may orally ask a client for permission to disclose PHI as described below, and the client has the opportunity to agree, limit or object to the disclosure. Disclosures based on a person's oral agreement are limited to the following:

   a. If the client is present for or available prior to a disclosure, P.H. employees may disclose to a family member, other relative, or a close personal friend of the client, the protected health information directly relevant to such person's involvement with the individual's health care or payment related to the individual's health care.

      When requesting permission to disclose PHI, the P.H. Employee must:

      i. Determine whether the client has the capacity to make a health care decision; and
      ii. Clearly explain the PHI intended to be disclosed; and
      iii. Provide the client with the opportunity to object to the disclosure; and
      iv. Make reasonable inferences based on professional judgment whether the client in fact agrees with the disclosure.

   b. If the client is not present or not capable of agreeing to the disclosure, the P.H. employee may exercise professional judgment to determine whether the disclosure is in the best interests of the client and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's care or payment related to the individual's health care or needed for notification purposes.

2. Disclosures in Correctional institutions [45CFR 164.512(k)]:

   Law Enforcement Medical Care (LEMC) employees may disclose minimally necessary PHI to a correctional institution or a law enforcement official having lawful custody of an inmate, for the purpose of providing health care or ensuring the health and safety of the inmate, other inmates, individuals, or the officers and employees of the correctional institution.

3. Uses and disclosures for disaster relief purposes

   SLOHA may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities to notify, or assist in the notification of (including identifying or locating), a family member*, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death.

4. Public health activities [45CFR 164.512]:

   Public Health employees who have been authorized by the Public Health Administrator may use and/or disclose PHI without an individual's authorization to carry out its duties as a public health authority.

G. Special Provisions for Disclosure of PHI in **Drug and Alcohol Services Programs**

Protected health information created, accessed, used and disclosed for clients applying for or receiving services from the SLOHA Drug and Alcohol Services (D&A) Division is subject to privacy rules in HIPAA [45cfr 164.500 – 164.534] *and* 42CFR Part 2. Together, these statutes place restrictions on the use and disclosure of PHI beyond those applicable to PHI in other SLOHA divisions.

1. Scope:

   Policy and procedure in this section applies to all employees who create, access, use or disclose protected health information related to clients in the SLOHA Drug and Alcohol Services Division.

2. Use and Disclosure of PHI in a Drug and Alcohol Program:

   a. Permitted use and disclosure of PHI in a Drug and Alcohol Program without an authorization is limited to:

      i. Mandatory disclosures as specified in this policy and procedure. (Child Abuse, Audit, Etc.)

      ii. Treatment purposes within the substance abuse treatment program and subject to minimum necessary standard. Note: Disclosure for any reason to other agencies including those within the Health Agency Umbrella of Care requires authorization.

      iii. Payment and operations purposes consistent with HIPAA statutes.

   b. Written Authorization (Referred to as "consent" in 42CFR Part 2)

      i. Other than uses and disclosures for "Treatment, Payment, or Healthcare Operations", and mandatory disclosures, SLOHA employees may not disclose any information about a client receiving services in a SLOHA drug and alcohol program without a written authorization.

      ii. Many clients in D&A programs require their PHI be disclosed to individuals or agencies outside of the Health Agency umbrella of care. These clients may concurrently be clients of the County Department, Social Services or County Probation Department or other agency. Employees must request that a client in a Drug and Alcohol Services program sign an applicable multi-party Authorization to Release Protected Health Information at the first visit or first incidence of service. This multi-party written authorization must include the names of all of the individuals who attend client meetings. If additional parties attend a future meeting, an updated multi-party release shall be signed by the client prior to the meeting.

   c. Additional confidentiality restrictions for Drug and Alcohol (D&A) Programs:

      i. Employees may not confirm information that an individual may already know about a client in a D&A program or that the employee believes may be known by the requester unless client written authorization is granted. [42CFR 2.13(b)]

ii. An employee may not acknowledge the presence or participation of an employee in a D&A program unless client written authorization is granted. [42CFR 2.13(c)]

iii. Disclosures of health information in the Drug and Alcohol Division to individuals outside of SLOHA shall only be performed by a Custodian of Records.

d. Specialized training

Within 30 calendar days of reporting for duty, all employees working in the Drug and Alcohol Services Division or working with D&A program PHI must read Part I, "The Regulations," of the book Confidentiality and Communication: A Guide to the Federal Drug and Alcohol Confidentiality Law and HIPAA (Legal Action Center). This book is available at all D&A treatment sites.

In addition, all D&A employees, and SLOHA employees or SLOHA contractor employees who have a need for working with D&A program PHI must attend a one-hour training on 42CFR, Part 2

3. Standards for Disclosure of D&A PHI

Disclosure of client information related to Drug and Alcohol treatment or prevention that contains information related to client identity, diagnosis, prognosis, or treatment may only be made based on the following table:

Guidelines for Authority to Disclose PHI in Drug and Alcohol Services		
Scenario	Staff Response	Comment
a) Client wants his or her record reviewed by the SLOHA Patient Rights Advocate (PRA), or PRA is investigating a complaint or monitoring client record for compliance.	Must Disclose	Authorization is not needed. PRA has authority designated by the DAS Manager for purposes of investigation/monitoring for compliance.
b) Original reporting of all mandated scenarios (elder/child abuse, Tarasoff, communicable diseases)	Must Disclose	Subsequent conversations are not permitted without authorization.
c) Clinician is communicating to a qualified professional in the course of conservatorship (Legal representative of the client.	May Disclose	Authorization is not needed. Limit the disclosure to “need-to-know-basis”.
d) Coroner’s office is requesting information to determine cause of death	May Disclose	Only permitted to report a death (H&S code 102850). 42CFR Section 2.15(b)(1) permits a limited disclosure about a deceased patient for an inquiry into the cause of death.
e) Clinician is referring the client to an Organizational Provider (health care services) contracted with the County Health Agency. (e.g. FCN, TMHA, CDC, Kinship) This includes ongoing communication for case coordination.	May Disclose w/ Authorization	FCN=Family Care Network TMHA=Transitions Mental Health Association CDC=Child Development Center
f) Clinician is communicating to a qualified professional who has or will assume medical or psychological responsibility for the care of the client.	May Disclose w/ Authorization	Authorization is needed. Ex: Discussing care with client’s current physician, or referral to a Network Provider who accepts the client.
g) Clinician is disclosing information pursuant to items (a,c,d,e) above that is part of the client’s record, but comes from other agencies or treatment providers (labs, Health and Physical, discharge summary). Does not include any alcohol/drug treatment records.	May Disclose w/ Authorization	Records that contain information about other clients or family members cannot be disclosed without a specific authorization from that other client or family member.
h) A relative or member of the general public (Or another agency member such as Probation, DSS, etc.) is asking for information about client care.	Must Not Disclose w/o Authorization	Authorization is required. Make sure the client is specific about what kind of information is permissible to disclose.
i) A professional who is not currently responsible for the care of the client (e.g. Client’s former doctor) is asking for information about the client	Must Not Disclose w/o Authorization	Authorization is required. Make sure the client is specific about what kind of information is permissible to disclose.
j) Information is requested regarding a deceased client.	Must Not Disclose	Authorization is required from the client’s Personal Representative.
k) Anyone seeking information about a sequestered record.	---	Consult with Compliance Officer or designated staff
l) Client’s attorney requests information.	---	Authorization is required.
m) Law enforcement is requesting information about a client.	---	Authorization is required.

H. Disclosures permitted only by Custodians of Records

NOTE: The following disclosures shall only be performed by a designated Custodian of Records. Such designees include Health Information Technicians as well as the designated Custodian of Records for Public Health, Mental Health, and Drug & Alcohol Services. Individuals disclosing PHI for the purposes below must refer to state/federal statutes (such as 45CFR 164.500 et al, W&I Code 5328 et al, and 42CFR Part 2)

1. To avert serious threat to safety [45CFR 164.512(j); W&I 5328(r); W&I 5328.3; W&I 5328.4; and 42CFR 2.12]:
(Public Health and Mental Health with narrow application in D&A)

   Subject to certain limitations, a custodian of records may disclose PHI for the purpose of averting a serious threat to if the employee believes in good faith the disclosure is necessary to:

   a. Prevent or lessen a serious and imminent threat to the health or safety of a person or the public, and to

   b. An individual(s) reasonably able to prevent or lessen the threat, including the target of the threat;

   The custodian of records must ensure that statutory requirements for authorization are met when making such disclosure.

2. Health oversight activities [45 CFR 164.512(d); W&I 5328; 42CFR 2.12]:
(All Divisions)

   SLOHA Management may disclose PHI without an authorization for health oversight activities authorized by law, including: audits, quality assessment, accrediting/licensing of health care professionals and plans, compiling and analyzing information in anticipation of a civil or criminal legal proceeding, case management and care coordination, business planning and development, resolution of internal grievances (i.e., reviewing allegation of improper conduct), resolution of disputes from clients, or other activities necessary for oversight of the health care system including:

   a. Government benefit programs for which health information is relevant to beneficiary eligibility;

   b. Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards;

   c. Entities subject to civil rights laws for which health information is necessary for determining compliance.

3. Judicial and administrative proceedings [45 CFR 164.512(e) W&I 5328; 42CFR 2.12]:
(Public Health, Mental Health in limited circumstances, D&A with Court Order only)

   SLOHA Management may disclose PHI without an authorization for judicial and administrative proceedings in response to an order of a court, subpoena, discovery request, or other lawful process unless prohibited, or otherwise limited, by federal or state law applicable to program or activity requirements.

4. Law enforcement purposes [45 CFR 164.512(f), and W&I Code 5328]:
(Public Health and Mental Health only)

   In limited circumstances, SLOHA Management may disclose PHI as allowed by HIPAA statutes and Welfare & Institutions Code 5328.

5. Decedents [45 CFR 164.512(g)]:
(Public Health or Mental Health)

   SLOHA Management may disclose PHI to a coroner or medical examiner to identify a deceased person, determine a cause of death, or other duties as authorized by law.

6. Research [45 CFR 164.512(i)]:
(All Divisions)

   SLOHA Management may disclose PHI for research purposes.

7. Specialized government functions [45 CFR 164.512(k)]:
(Public Health only)

   SLOHA Management may disclose PHI for specialized government functions, including authorized federal officials for conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by law.

8. Programs Providing Public Benefits (k)(6)(ii)
(Public Health Only)

   Programs administering a government program providing public benefits may disclose PHI relating to the program to another covered entity that is a government agency administering a government program providing public benefits if the programs serve the same or similar populations and the disclosure of PHI is necessary to coordinate the covered functions of such programs or to improve administration and management relating to the covered functions of such programs.

I. Accounting and Logging of Disclosures

1. All disclosures of PHI outside of the Health Agency umbrella of care must be recorded in the client's health records either electronically, *or if in a paper record*, with a Record of Disclosure Form (Under Development) with the following exceptions:

   a. Disclosures requested by the client to themselves.

   b. Social Workers who are authorized by the Courts to have custody or care of a minor.

   c. Common mandatory disclosures.

      i. Tarasoff Warning
      ii. Child or Elder/Dependent Adult Abuse Reports
      iii. Firearm Injury
      iv. Breach Reports

   d. Certain disclosures limited to the Psychiatric Health Inpatient Unit.

2. Guidance for logging of disclosures in the Drug and Alcohol Services Division can be found on the intranet or by clicking here: Policy B9-100.0 D&A Authorization to Disclose PHI.

3. Guidance for logging of disclosures in the Public Health Department can be found in HIPAA statute 45CFR 164.528.

4. Guidance for logging of disclosures in the Mental Health Division can be found on page 60 of the Treatment Plans and Documentation Guidelines.

ATTACHMENT A:

REQUIRED ELEMENTS OF AN AUTHORIZATION TO RELEASE PHI FORM

NOTE: This form may be used to ensure that an authorization form from a non-county provider meets the regulatory standards for a legal client authorization.

Authorization forms may not be combined with any other document (e.g., consent for treatment forms) to create a "compound authorization." The authorization form must be must be on 8 ½ x 11-inch paper and the font size must be at least 14 points.

HIPAA, state law, and SLOHA policy and procedure require that each client's authorization include certain core elements as follows:

J. Client's name and date of birth

K. Name of the disclosing entity/facility

L. Name and address of the facility/individual to receive the protected health information

M. Description of the information to be disclosed

N. Description of the purpose of the disclosure

O. Expiration date or the condition upon which authorization is terminated

P. The client's initials must be shown next to the types of PHI being released in a "protected classes" section for release of:

   1. mental health information,
   2. substance abuse information,
   3. HIV/AIDS information,
   4. developmental disabilities,
   5. sexually transmitted disease information.

Q. Completed statements where client acknowledges the following:

   1. I understand that authorizing the disclosure of this health information is voluntary. I may refuse to sign this authorization.
   2. I understand that I may not be denied treatment, payment, enrollment in a health plan or eligibility for benefits if I refuse to sign.
   3. I understand that I have a right to receive a copy of this authorization.
   4. I understand that my authorization to use or disclose protected health information expires on _____ or until _____ condition is met.
   5. I understand that I may cancel my authorization at any earlier time by writing a note of cancellation and giving it to _____. I also understand that when I give or cancel my authorization, it is effective from that date and time forward, and not retroactively.
   6. I understand that information disclosed as a result of this authorization could be re-disclosed by the recipient. Such re-disclosure is in some cases not protected by California law and may no longer be protected by federal confidentiality law.

R. Signatures and Dates

   1. Client
   2. Parent/Guardian/Conservator if client is unable to sign
   3. Witness, if client is unable to sign

Subpoenas, Court Orders and Warrants

I. PURPOSE

These policies and procedures are intended to ensure compliance with statutes, regulations and contractual obligations that govern the privacy and confidentiality of health information created, maintained, accessed and stored by the San Luis Obispo County Health Agency (SLOHA)

This policy and procedure addresses the appropriate handling of subpoenas, court orders, and warrants.

II. SCOPE

This policy and procedure document applies to all individuals who may access, use, or disclose SLOHA PHI that is created, accessed, used or disclosed by the San Luis Obispo County Health Agency.

This policy and procedure is applicable to protected health information and other protected information created, accessed, used and disclosed for clients requesting or receiving treatment in SLOHA alcohol and drug programs, mental health programs and public health programs.

III. DEFINITIONS

A. Court Order: A Court Order is a writ issued by a court of law requiring a person to do something or to refrain from doing something

B. Subpoena for documents: (also known as a Subpoena Duces Tecum) A Subpoena is a legal process to demand the production of documents or other tangible evidence.

C. Warrant: A legal document authorizing an officer to make an arrest, seize property, or conduct a search.

D. Special Master: A specially appointed attorney who has been assigned by the courts to accompany the person serving a search warrant.

IV. POLICY

A. General Policy

1. Only SLOHA supervisors, managers or Custodian of Records staff may disclose information requested pursuant to a subpoena, court order, or warrant. Disclosure shall be consistent with the SLOHA Subpoena Procedure Handbook.

2. The Health Agency shall to the extent allowed by law, comply with all court orders.

3. Compliance with subpoenas and warrants shall be consistent with legal statutes and at the discretion of SLOHA management.

4. NOTE: Information that is privileged or confidential under the law, such as information related to Drug and Alcohol Services clients, must not be disclosed without either the client's authorization or a court order. See "Special Handlings" below for guidance.

B. Court Orders

1. To the extent allowed by law, court orders supersede all regulations and must be complied with. A court order may be presented by law enforcement to search a premises or program, arrest a client, or demand documents.

2. Court orders related to Alcohol and Drug programs must comply with 42CFR section 2.63 – 2.67 in order to be valid.

3. Upon receipt of a court order, employees must immediately provide it to a supervisor, manager or Custodian of Records for processing. If a supervisor or manager is not available, employees shall request that the person with the Court Order return when a person of authority is available. If the person executing the court order refuses to comply, ensure that the court order is valid and comply with the order.
4. If the Health Agency is unable to comply with a court order because it does not meet statutory requirements, it is essential that we respond to the courts through appropriate legal means.

C. Subpoena

NOTE: Information that is privileged or confidential under the law, such as information related to Drug and Alcohol Services clients should not be disclosed without either the individual's Authorization or a court order. See “Special Handlings” section below for additional guidance.

1. Protected health information may be disclosed in response to a subpoena, discovery request, or other lawful process, without a court order, if one of the following circumstances applies:
   a. The client signs an Authorization to Disclose Protected Health Information; or
   b. The disclosure is permitted by state or federal statute; *and*
      i. The County receives satisfactory assurances from the party seeking the protected health information that reasonable efforts have been made to ensure that the individual who is the subject of the protected health information has been given notice of the request for protected health information; or
      ii. The County receives satisfactory assurance from the party seeking the protected health information that reasonable efforts have been made to secure a qualified protective order.
2. If presented with a subpoena, employees must bring it immediately to a supervisor, manager, or a Custodian of Records.
3. Additional procedures apply for handling and processing a subpoena at Subpoena Procedure.
4. If the Health Agency is unable to comply with a subpoena, it is essential the response is through appropriate legal means such as County Counsel.

D. Coroner’s Subpoenas

1. Coroner’s Subpoenas are requests for information generated by the Coroner. No PHI from clients in a Drug and Alcohol Program or Mental Health Program may be disclosed pursuant to a Coroner’s subpoena. (Note: Law enforcement may cite Civil Code 56.10 as the grounds for disclosure to the Coroner, however Civil Code 56.30(a) and 56.30(i) specifically exempt mental health and drug and alcohol programs from the entirety of Civil Code 56.)
2. Disclosures of PHI in Public Health programs pursuant to a Coroner’s Subpoena are permitted, but are not mandatory.

E. Warrants for Records

NOTE: Information that is privileged or confidential under the law, such as information related to Drug and Alcohol Services clients should not be disclosed without either the individual's authorization or a court order. See “Special Handlings” section below for additional guidance.

1. Employees presented with a valid warrant by a law enforcement officer shall immediately notify a supervisor, manager, or Custodian of Records.
2. SLOHA employees shall comply with law enforcement officials serving an arrest warrant on a client in a mental health or public health program. (See special handling for Alcohol and Drug programs.)
3. SLOHA employees shall comply with law enforcement officials serving a search warrant on a mental health or public health program to the extent authorized in the search warrant, but in no case may protected health information be released unless authorized by state and federal statutes including 45CFR 164.500- 164.534 and California Welfare and Institutions Code 5328 – 5330. (See special handling for Alcohol and Drug programs.)

F. Special Handlings

1. HIV/AIDS records, DNA records, or other protected records
   a. PHI related to a client’s HIV/AIDS condition or treatment, PHI related to the individual's DNA, or other specially protected records such as dental records may not be disclosed without a Court Order unless it is de-identified.
   b. Employees shall immediately notify a supervisor, manager or Medical Records staff of the subpoena. If the Health Agency is unable to comply with a subpoena, it is essential that we respond through appropriate legal means.
2. Alcohol and Drug programs

   PHI related to a client’s treatment or request for treatment in an Alcohol and Drug program may only be released through a court order that is compliant with 42CFR Part 2, Section 2.63 – 2.67, or though client authorization.
3. Subpoena

   If a subpoena for records is received, employees shall immediately notify a supervisor, manager or Medical Records staff of the subpoena. The Medical Records section has special procedures for responding to Subpoenas. See Subpoena Procedures.
4. Arrest and Search Warrants in Drug and Alcohol Services

   NOTE: The below guidance on arrest and search warrants does not apply if an officer has an arrest warrant for a client who has committed or threatened to commit a crime on the SLOHA D&A program premises or against SLOHA D&A program personnel.

   If a law enforcement officer presents a warrant to search the premises, to seize documents or to arrest a client, in our Alcohol and Drug programs, employees must act with urgency to notify management. The following procedure should be followed if a law enforcement officer seeks to search the premises, seize documents or arrest a client, in our Alcohol and Drug programs:

   a. Produce a copy of 42CFR Part 2 and explain that the County cannot cooperate with a search or arrest warrant without an appropriate court order issued in accordance to the regulations.

b. Contact County Counsel and ask for immediate assistance with the matter.

c. Ask to contact the prosecuting attorney or commanding officer if earlier attempts at explaining the County's position fail.

d. If the officer insists on entry, **do not forcibly resist**.

V. APPLICABLE STANDARDS/REGULATIONS

- HIPAA 45 CFR 164.100 – 164.534
- H&S 5328 – 5328.9
- 42 CFR, Part 2
- California Civil Code 56.10 – 56.11
- H&S 123100-

San Luis Obispo County Health Agency

Health Information Privacy and Security Policy and Procedure Suite

Chapter 2
Information Security Policies & Procedures

Organization, and General Policies

(Security Policy and Procedure #1)

II. PURPOSE

These policies and procedures are intended to ensure compliance with statutes, regulations and contractual obligations that govern the security of health information created, maintained, accessed, and stored by the San Luis Obispo County Health Agency.

III. SCOPE

This policy and procedure document applies to the privacy and security of all protected health information controlled by the County Health Agency regardless of form or media.

This policy and procedure document applies all employees, contractors, agents or volunteers (hereinafter: Employees) of the San Luis Obispo County Health Agency.

IV. DESIGNATION OF ASSIGNED SECURITY RESPONSIBILITY

Pursuant to 45 CFR 164.308(a)(2), the Health Agency Director shall designate a HIPAA Security Officer responsible for oversight of this policy and procedure suite as well as compliance with the HIPAA Security Rule.

Responsibilities for The HIPAA Security Officer include but are not limited to:

- Develops and maintains policies, procedures and standards that provide adequate integrity, security and availability of electronic personal health information (ePHI) for all Health Agency HIPAA covered components.
- Deploys and maintains provided system resources designed to protect the integrity, security and availability of ePHI for all Health Agency HIPAA covered components.
- Directs risk/vulnerability assessments, system audit activity, system access review, system patch and maintenance activities.
- Coordinates incident response, contingency planning and disaster recovery.
- Acts as primary expert on protected health information including ePHI as defined by HIPAA statutes.

V. ORGANIZATION

This Health Information Security Policy and Procedure is a suite of documents designed to comply with the various statutes, regulations and contractual obligations that govern the security of health information created, maintained, accessed, and stored by the San Luis Obispo County Health Agency. Included are those HIPAA statutes regulating the security of electronic protected health information (ePHI). This section of the HIPAA regulation is commonly known as Subpart C or the HIPAA Security Rule. The policies included in this suite are organized by topic and address the requirements and standards set forth in the HIPAA security rule, (45 CFR 164.302-164.318 - Subpart C – Health Insurance Portability and Accountability Act (HIPAA) Security Standards) and other related statutes. For the purposes of this policy and procedure document, ePHI shall at a minimum include all protected electronic health information as defined by HIPAA statutes.

VI. POLICY

A. The Health Agency shall develop and maintain policies, procedures and forms for the purposes of securing ePHI as mandated by HIPAA statutes and/or other regulations or contractual agreements.

B. The Health Agency shall develop and maintain documentation of actions, activities or assessments as required, which demonstrate compliance with related statutes. Such documentation shall be retained for a minimum of six years. Documentation may be retained longer if required by state law or licensing requirements.

C. Documentation, policies and procedures shall be available to employees responsible for implementing the policies and procedures contained herein.

D. Documentation, policies and procedures shall be reviewed periodically and updated to address changes in statute, or to address operational, technology or environmental changes that affect security of ePHI.

VII. CONFLICT WITH OTHER SECURITY LAWS

A. SLOHA has adopted reasonable policies and procedures for the administration of its programs, services, and activities. If any state or federal law or regulation or order of a court having appropriate jurisdiction, imposes a more stringent requirement related to the privacy of confidential information, SLOHA shall act in accordance with the standard requiring stricter protection from disclosure or more permissive access to the client.

B. In the event more than one policy applies, and compliance with all such policies cannot be reasonably achieved, SLOHA employees shall seek guidance from an immediate supervisor or the HIPAA Privacy Officer.

VIII. APPLICABLE STANDARDS/REGULATIONS

- 45 CFR sections 164.302 – 164.318 (The Security Rule) details rules governing the security of ePHI.
- 45 CFR 164.308(a)(2) which sets forth the requirement to designate a HIPAA Security Officer.
- 45 CFR 164.316 which sets forth the rules for maintaining policies, procedures and documentation

Risk Assessment and Management

(Security Policy and Procedure #2)

I. PURPOSE

This policy and procedure is intended to ensure compliance with HIPAA statutes and other regulations requiring risk assessment and risk management in identifying and addressing vulnerabilities to the confidentiality, integrity and availability of ePHI

II. SCOPE

This policy and procedure document applies to the privacy and security of all ePHI controlled by the County Health Agency regardless of form or media.

III. POLICY

The County Health Agency's covered components shall conduct periodic assessments of risks and vulnerabilities to the confidentiality and availability of ePHI. When risks or vulnerabilities are identified, remediation measures will be considered and adopted as necessary to comply with statutes.

A. Risk Assessment

1. An overall ePHI security program assessment shall be conducted periodically, but no less than every two years on key components of the County HIPAA security policy.
2. A targeted risk assessment shall be conducted when the following events occur:
    a. Adoption of new system applications or modification of existing system applications that contain or protect ePHI.
    b. Material modifications to existing facilities or development of new facilities that house ePHI or where ePHI is accessed.
    c. Material changes to policy or development of new policies related to the privacy and security of ePHI.

B. Risk Management

Security measures and controls shall be considered and implemented as necessary to comply with applicable statutes. Such measures include:

1. Implementing access controls, authorization and validation procedures
2. Conducting detection and activity audits
3. Implementing training and change management processes
4. Implementing incident reporting and response procedures
5. Establishing or modifying contingency, data backup, and disaster recovery plans
6. Imposing sanctions for non-compliance
7. Creation or modification of Policy and/or Procedure
8. Technology Controls including:
    a. Installation, update or removal of network services and components.
    b. Installation of operating systems upgrades
    c. Installation, update or removal of applications, software and database servers.

IV. APPLICABLE STANDARDS

- 45 CFR 164.308(a)(1)(ii)(A) requires that covered entities conduct an assessment of risks and vulnerabilities to the confidentiality and availability of ePHI.
- 45 CFR 164.308(a)(1)(ii)(B) requires that covered entities implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.
- 45 CFR 164.308(a)(8) requires that covered entities perform periodic technical and non-technical evaluation of procedures and systems protecting the security and integrity of ePHI.

Sanctions for Violation of Policy/Procedure

(Security Policy and Procedure #3)

I. PURPOSE

This policy and procedure is intended to ensure compliance with HIPAA statutes and other regulations that require sanctions to be considered against employees, contractors, agents or volunteers who fail to comply with the security policies and procedures contained herein.

II. SCOPE

This policy and procedure document applies to the privacy and security of all ePHI controlled by the County Health Agency regardless of form or media.

This policy and procedure document applies all employees, contractors, agents or volunteers of the San Luis Obispo County Health Agency.

III. POLICY

A. Disciplinary Actions and Sanctions

An employee of the Health Agency who violates any provision of the County's HIPAA privacy or security policies and procedures shall be subject to disciplinary actions up to and including termination of employment. An agent, volunteer or contractor of the County Health Agency who violates any provision of the Health Agency's HIPAA privacy or security policies and procedures shall be subject to sanctions which may include but are not limited to contract cancellation or termination of services.

B. Obligation to Report Violations

An employee, agent or volunteer of the Health Agency who has a reasonable belief that the County's HIPAA privacy or security policies and procedures have been violated must report the violation to their supervisor, manager, department HIPAA Privacy Officer, or the department HIPAA Security Officer immediately. HIPAA regulations require the County to report select violations to the Department of Health Care Services within 24 hours. As such, immediate reporting is essential to meet this statutory timeline. The violation must be reported whether committed by the person reporting the violation, or another individual and it must be reported whether intentional or accidental.

C. Prohibition Against Retaliation

Retaliation against any person who in good faith reports a violation of the Health Agency's HIPAA privacy or security policies and procedures or retaliation against any person who supports someone else who reports a violation of the policy is prohibited. In addition, retaliation against any person who cooperates in an investigation related to this policy is prohibited.

IV. APPLICABLE STANDARDS/REGULATIONS

- 45 CFR 164.308(a)(1)(ii)(C) requires that covered entities apply sanctions against workforce members who fail to comply with the security policies and procedures contained herein.

Security Incident Response and Incident Reporting

(Security Policy and Procedure #4)

I. PURPOSE

This policy and procedure is intended to ensure compliance with HIPAA statutes and other regulations that require a covered entity to respond to and document suspected or known security incidents and mitigate harmful effects to the extent practicable.

II. SCOPE

This policy and procedure document applies to the privacy and security of all ePHI controlled by the County Health Agency regardless of form or media.

This policy and procedure document applies all employees, contractors, agents or volunteers of the San Luis Obispo County Health Agency.

III. POLICY

Any known security incidents that are related to or affect the privacy, confidentiality or integrity of ePHI shall be identified, reported, and documented. In addition, the Health Agency shall identify any harmful effects of a security issue and mitigate those harmful effects to the extent practicable. Reporting responsibility is as follows:

A. Employee, Contractor, Agent or Volunteer Reporting

An employee, agent or volunteer of the Health Agency who has a reasonable belief that the County's HIPAA privacy or security policies and procedures have been violated must report the violation to their supervisor, manager, department HIPAA Privacy Officer, or the department HIPAA Security Officer immediately. Regulations require the County to report select violations to the Department of Health Care Services within 24 hours. As such, immediate reporting is essential to meet this statutory timeline. The violation must be reported whether committed by the person reporting the violation, or another individual and it must be reported whether intentional or accidental.

B. Supervisor and Manager Reporting

A supervisor or Manager who is made aware of a security incident, threat or vulnerability under this policy shall report the incident to a designated HIPAA Privacy Officer or the HIPAA Security Officer.

C. All reports of a HIPAA related incident involving ePHI must be logged by the HIPAA Security Officer on the HIPAA Incident Log.

IV. PROCEDURE

A. Incident or Threat Assessment

Upon receiving a report of a security incident or threat, the HIPAA Privacy Officer or HIPAA Security Officer shall assess the nature of the incident using the Health Agency Incident Assessment and Mitigation Report. The Officer may seek advice further advice from the Health Agency Director or designee, County Information Technology, County Counsel, or may seek to convene the Health Agency Compliance Steering Committee.

B. Response and Mitigation

1. If the matter can easily be corrected and mitigated, the Officer completing the report will take necessary steps to correct the incident and will document the steps taken on the Health Agency Incident Assessment and Mitigation Report. A copy of the final report shall be provided to the HIPAA Security Officer.

2. If the reported incident requires resources, expertise or authority beyond that of the HIPAA Privacy Officer or HIPAA Security Officer, the Officer may seek advice further advice from the Health Agency Director or designee, County Information Technology Department, County Counsel, or may seek to convene the Health Agency Compliance Steering Committee. Mitigating measures will be assessed and implemented where appropriate and consistent with statute. A copy of the final Health Agency Incident Assessment and Mitigation report shall be provided to the HIPAA Security Officer.

C. Incident Logging

All reports of a security incident or threat shall be logged on the HIPAA Incident Log. All incident reports shall be supported by a completed Health Agency Incident Assessment and Mitigation report.

D. Additional Contacts

Employees may also contact the following if they are aware of or suspect violation of these policies or applicable regulations:

- You can call the toll-free confidential hotline at: **(855) 326-9623**
- Or you can contact us by e-mail at: privacy@co.slo.ca.us
- Or send a letter to:
  Privacy Officer
  San Luis Obispo County Health Agency
  2180 Johnson Avenue
  San Luis Obispo, CA 93401

You may also contact the Department of Health and Human Services at:

Office of Civil Rights
90 7th Street, Suite 4-100
San Francisco, CA 94103

- Or you can file a complaint online at: www.hhs.gov/ocr/privacy/hipaa/complaints
- Or call toll free at: (800) 368-1019 - TDD (800) 537-7697

V. APPLICABLE STANDARDS/REGULATIONS

- 45 CFR 164.308(a)(6) requires that covered entities respond to and document suspected or known security incidents and mitigate harmful effects to the extent practicable.
- AB 1149 amending Section 1798.29 of the California Civil Code.

VI. RESOURCES

A. Incident Report Form (For Employee Use)

B. Compliance Officer's Breach Risk Assessment Form (Restricted Access – M:/QST)

C. DHCS Privacy Incident Report Form (Restricted Access – M:/QST)

D. Incident Log (Restricted Access – M:/QST)

Business Associates

(Security Policy and Procedure #5)

I. PURPOSE

This policy and procedure is intended to ensure compliance with HIPAA statutes requiring covered entities to obtain assurances in the form of contract or other arrangement that a Business Associate will safeguard ePHI and will require their subcontractors to safeguard ePHI consistent with HIPAA statutes.

II. SCOPE

This policy and procedure document applies to relationships between the County and any entity acting in the capacity of a Business Associates as defined by HIPAA statutes.

III. POLICY

1. All entities doing business with the Health Agency and acting in the capacity of a Business Associate as defined by HIPAA statutes shall execute a Business Associate Agreement with the County.

   NOTE: If unsure about whether an entity doing business with the Health Agency is a Business Associate, employees must consult with the HIPAA Privacy Officer or the Compliance Program Manager.

2. County employees who receive a report or complaint from any source about inappropriate safeguards to ePHI by Business Associates shall report the matter to supervisor, manager, department HIPAA Privacy Officer, or the department HIPAA Security Officer consistent with section III. (B) of Sanctions for Violation of Policy/Procedure

IV. PROCEDURE

A. Determination of Business Associate Status

1. All proposed or renewed business relationships between third-party entities and the County, (that are administered by the Health Agency), shall be reviewed for Business Associate status using the Business Associate Decision Tool, prior to executing an agreement with the entity.

2. If the business relationship qualifies for Business Associate status, a Business Associate Agreement (BAA) shall be prepared and included in the contract signed by the Business Partner Entity.

B. The employee responsible for administering the contract and agreement with the Business Associate will secure appropriate signatures and include the BAA with the contract for Board approval or Health Agency Director Approval. Upon approval by the Board or Health Agency Director, a copy of the executed BAA will be provided to the Privacy Officer.

C. The Privacy Officer will record the agreement into the Business Associate log.

V. APPLICABLE STANDARDS/REGULATIONS

- 45 CFR 164.308(b)(1) -164.308(b)(3) requires covered entities to obtain assurances in the form of contract or other arrangement that a Business Associate will safeguard ePHI and will require their subcontractors to safeguard ePHI consistent with HIPAA statutes.

VI. RESOURCES

A. Business Associate Agreement Decision Tool (Form) / Business Associate Log

Security Awareness and Training

(Security Policy and Procedure #6)

I. PURPOSE

This policy and procedure is intended to ensure compliance with HIPAA statutes and other regulations requiring covered entities to implement a security awareness and training program which includes periodic security updates.

II. SCOPE

This policy and procedure document applies to the privacy and security of all ePHI controlled by the County Health Agency regardless of form or media.

This policy and procedure document applies all employees, contractors, agents or volunteers of the San Luis Obispo County Health Agency.

III. POLICY

A. The Health Agency will conduct periodic training for the purposes of protecting ePHI and complying with HIPAA statutes. This training shall at a minimum include:

1. New hire training on HIPAA privacy and security within 60 days of assuming their position for any individual who is new to the Health Agency and is working with ePHI.

2. New hire training on HIPAA privacy and security within 60 days of assuming their position for any individual who is reassigned to a position within the Health Agency that works with ePHI and has not received HIPAA privacy and security training within the previous 12 months.

3. HIPAA privacy and security update training annually for all employees of the Health Agency who work with PHI or ePHI.

B. The Health Agency shall have a Security Awareness Program that raises employee awareness of PHI and ePHI privacy and security. The awareness program shall at a minimum include related employee literature posted at every Health Agency worksite and a semi-annual security update letter to all Health Agency employees.

C. Training records shall be maintained for a minimum of six years.

IV. APPLICABLE STANDARDS/REGULATIONS

- 45 CFR 164.308(a)(5) requires covered entities to implement a security awareness and training program which includes periodic security updates.

User Access, Authentication and Password Management

(Security Policy and Procedure #7)

I. PURPOSE

This policy and procedure is intended to ensure compliance with HIPAA statutes and other regulations requiring covered entities to specify who access to ePHI is granted, managed, monitored, and authenticated.

II. SCOPE

This policy and procedure document applies to the privacy and security of all ePHI controlled by the County Health Agency regardless of form or media.

This policy and procedure document applies all employees, contractors, agents or volunteers of the San Luis Obispo County Health Agency.

III. POLICY

A. Level of Access

The Health Agency shall maintain a matrix defining level of access for individuals by classification or position. Modifications to the matrix may only occur after approval by the Health Agency Director.

B. Granting or Modifying User Access

The following applies when granting or modifying access to systems containing ePHI:

1. Initial requests or requested modifications for individual access to ePHI systems shall be submitted to the HIPAA Security Officer by the employee's supervisor, Departmental Personnel Technician, or other authorized individual.
2. Access to ePHI shall not be granted to any person prior to reading and signing an Oath of Confidentiality.
3. Access to ePHI shall not be granted to any person who has not passed a pre-employment background check for their classification pursuant to the County Employee Background Check Policy.
4. Access to ePHI shall not be granted to any person prior to ensuring the person is not on the Excluded Provider List of the Office of the Inspector General.
5. All individuals with new access to ePHI must be trained within five working days of receiving access on basic system use and security of ePHI.

C. Termination or Suspension of Access

The following applies when terminating or suspending access to systems containing ePHI. (NOTE: Situations requiring termination or suspension of access may require a high level of urgency to protect ePHI, especially if the termination or suspension is involuntary).

1. Upon separation of an employee from County employment, access to systems containing ePHI shall be terminated within 24 hours. Special urgency shall be exercised when the separation is involuntary.
2. Change of Duties / Department: Access to ePHI shall be terminated for any employee whose duties have changed and no longer require access to ePHI or for any employee who has moved to a department outside of the Health Agency.

3. Leave of Absence: Access to ePHI shall be suspended for any employee on a leave of absence beyond 20 working days.
4. Investigation: At management's discretion, access to ePHI shall be suspended for any employee who is being investigated for misconduct.

D. Emergency System Access

1. When in the best interest of the client, management may grant access to ePHI to an individual who may not otherwise have access or who has not met all of the requirements for access described in this policy and procedure document.
2. The Security Officer shall maintain procedures for granting emergency access to ePHI.

DI. User Authentication and Password Management

Information systems used to access ePHI shall uniquely identify and authenticate any system user. All system users shall protect their password and comply with the password standards described in the Password and Authentication Policy (Pg 40-43).

DII. Log-in Monitoring

The Security Officer shall maintain and test procedures designed to monitor log-in attempts for all systems providing access to ePHI.

DIII. Automatic Logoff

All systems that access ePHI must have controls in place that log a user off the system after no more than 10 minutes of inactivity. All workstations that have access to ePHI must have controls in place that lock the screen after no more than 5 minutes of inactivity at that workstation.

IV. PROCEDURE

A. Level of Access

1. A matrix shall be maintained by the Security Officer identifying which classifications and/or positions within the Health Agency may have access to ePHI. Such matrix shall also include the level of access or activity (read only, edit, reporting, etc) each classification or position may have.
2. Requests for revisions to the matrix shall be submitted in writing to the Security Officer who will consult with the appropriate Privacy Officer to determine whether the requested revision shall be granted. A recommendation for approval or denial of the request shall be provided by the Security Officer to the Health Agency Director for final determination. Notification of determination shall be provided in writing to the individual requesting the revision and shall be maintained with the authorization matrix.

B. Granting or Modifying User Access

1. Initial requests for access to ePHI or requested modifications of access to ePHI must be submitted in writing to the Security Officer who may grant access to individual users consistent with the security matrix. Requests shall be submitted via the ePHI Add/Change Access Form and shall not be submitted until after the employee signs the Health Agency Oath of Confidentiality. Where do we document level of access by user?

2. All individuals with new access to ePHI must be trained within five working days of receiving access on basic system use and security of ePHI. Such training shall minimally include:
    a. Appropriate use and disclosure of ePHI.
    b. How to properly secure their workstation including procedures to log on and log off of the system and how to lock their work station.
    c. Instructions for notifying a supervisor or Security Officer when ePHI may have been altered or destroyed.
    d. Reporting a suspected or actual security breech.
    e. Logoff and screen-lock standards

C. Termination or Suspension of User Access

1. Requests for termination or suspension of access should be made in writing via the ePHI Add/Change Access Form; however verbal requests may be made when urgent action is warranted.
2. Any manager or supervisor may request suspension of access to ePHI. The Security Officer shall assess all requests for reasonableness and urgency.

D. Emergency System Access

When emergency access to ePHI has been granted to an individual who may not otherwise have access or who has not met all of the requirements for access described in this policy and procedure document, the following procedure must be adhered to.

1. The Health Agency Director, Health Officer or Behavioral Health Director may authorize emergency access to ePHI when they determine it is in the best interest of the client.
2. If emergency access is granted, the authorizing manager shall document the authorization within 48 hours of granting access. The documentation may be an e-mail to the HIPAA Security Officer who shall maintain the documentation.
3. After the need for emergency access is over, the user access shall be removed or the person receiving access shall complete the requirements for normal access within 15 working days.

E. Person or User Authentication

1. Person or entity authentication is achieved by way of a unique active directory ID for each user authenticated by a confidential and secure password known only to the user. All system users are assigned a unique active directory ID to access the network. All system users are responsible for creating and maintaining the confidentiality of the password associated with their unique user ID. Managers/supervisors are required to ensure that their staff understands the user responsibilities for securely managing confidential passwords.
2. Describe standard for securing passwords on encrypted server and how we generate unique user IDs

F. Log-in Monitoring

Software designed to monitor log-in attempts will be set to notify the Security Officer and designee when a user has multiple unsuccessful log-in attempts. The Security Officer shall investigate any activity believed to be suspicious and shall contact the supervisor of individuals who may need additional system training. The log-in monitoring system software shall be tested annually and documentation of results shall be maintained.

G. Password Management

For guidance on maintaining strong passwords, see the Information Security Program Password and Authentication Policy.

1. Upon receipt of a user ID, the person assigned the user ID is required to change the password provided by the administrator to a password that only he or she knows. Effective passwords shall be created in order to secure access to electronic protected health information (ePHI).
2. Employees who suspect their password has become known by another person shall change their password immediately. No user shall share his or her password with another person.
3. Employees are required to change their network user ID passwords every 90 days; when the technology is capable, each application access password shall be changed every 90 days. Where technology is capable, network and application systems shall be configured to enforce automatic expiration of passwords.
4. All passwords are to be treated as sensitive, confidential. Managers and supervisors who require emergency access to a worker's email or individual network drive shall reference the "emergency access" section of the County's HIPAA User Access Management policy.

V. APPLICABLE STANDARDS/REGULATIONS

- 45 CFR 164.308(a)(3) requires covered entities to implement policies to specify which employees shall have access to ePHI and implement procedures for determining level of access for individual users. In addition this section requires procedures for termination of access.
- 45 CFR 164.308(a)(4) requires covered entities to implement policies and procedures for conducting and implementing the authorization process. In addition this section requires identifying who is responsible for granting, modifying or terminating access and determining level.
- 45 CFR 164.308(a)(5)(ii)(C)- 164.308(a)(5)(ii)(D) requires covered entities to implement technologies for tracking logon attempts, and implement policies and procedures for creating, changing, and safeguarding passwords.
- 45 CFR 164.312(a)(2)(i) - 164.312(a)(2)(iii) requires covered entities to implement policies and procedures to assign unique access to ePHI by individual user, for access to ePHI in case of emergency, and for automatic logoff of access after user inactivity.
- 45 CFR 164.312(d) - requires covered entities to implement procedures that verify an individual seeking access to ePHI is the one claimed.
- 45 CFR 164.312(c) - 164.312(d) requires covered entities to implement policies and procedures to protect ePHI from improper alteration or destruction.

Workstation Security

(Security Policy and Procedure #8)

I. PURPOSE

This policy and procedure is intended to ensure compliance with HIPAA statutes and other regulations requiring covered entities to ensure workstations are configured, positioned, secured and used in a manner that protects from unauthorized disclosure of ePHI.

II. SCOPE

This policy and procedure document applies to the all workstations used or controlled by the County Health Agency regardless of form or media.

This policy and procedure document applies all employees, contractors, agents or volunteers of the San Luis Obispo County Health Agency.

III. POLICY

Use of all Health Agency workstations shall at a minimum be consistent with the County IT Acceptable Use Policy and County Information Security Program Policies. In addition, the following policies apply:

A. Authorized Use

Employees shall access only that data to which they have authorization and have a need to know. No employee shall access or attempt to access data for which they do not have authorization.

B. Automatic Workstation Lockout / Logoff

1. All workstations used by employees with access to ePHI and assigned to HIPAA covered components of the Health Agency shall be set to automatically "session-lock" after a period of inactivity. Such period shall not exceed 10 minutes with a recommended inactivity timeout of 5 minutes.

2. Employees shall manually lock their workstation using 'Windows key + L' or 'Ctrl-Alt-Delete' when the workstation is left unattended for any period of time.

C. Workstation Positioning

1. Employees shall ensure that observable confidential information is adequately shielded from unauthorized disclosure and unauthorized access on computer screens. This may include using polarized screens or other shielding devices. Employees shall make every effort to ensure confidential information on computer screens is not visible to unauthorized persons.

2. Workstations shall be installed in locations and positions so that their input devices, such as keyboard and mouse cannot be easily touched or used by unauthorized persons.

3. Health Agency employees assigned to County facilities not controlled by the Health Agency shall be aware of their surroundings to ensure no one can incidentally view ePHI and no ePHI is left unattended. Additional caution shall be applied when using a laptop, PDA or tablet.

D. Offsite Access to ePHI

Employees who work from home or other non-office sites shall take the necessary precautions to ensure protection of ePHI. This includes password protection of personal computers and security for all mobile devices storing ePHI such as locking up CD or DVD Disks, USB drives, PDAs, laptops and tablets.

E. Workstation Software

1. Employees shall only install software that has been approved by their supervisor and the HIPAA Security Officer on computers owned or operated by the Health Agency.
2. Health Agency IT shall monitor all logins to workstations and applications including failed logon attempts.

F. Data Storage on Workstation (C-Drive)

1. Employees shall not store ePHI on a workstation C-Drive (or other internal hard drive) without the consent of their manager or supervisor and approval of the HIPAA Security Officer who shall document the authorization including the business reason for storing ePHI on a local workstation drive.
2. In cases where ePHI has been stored on a workstation C-Drive, it shall be fully deleted or removed as soon as the need for the data ends. Removal includes permanent deletion from electronic trash cans.

IV. APPLICABLE STANDARDS/REGULATIONS

- 45 CFR 164.310(b)-164.310(c) requires covered entities to implement policies and procedures specifying appropriate use of a workstation to ensure security of ePHI as well as standards for how the workstation shall be physically protected to ensure security of ePHI.

- 45 CFR 164.312(a)(2)(iii) requires covered entities to implement policies and procedures for logging off when workstation is unattended and for automatic locking after a period of inactivity.
  -

Mobile Device Security

(Security Policy and Procedure #9)

I. PURPOSE

This policy and procedure is intended to ensure compliance with HIPAA statutes and other regulations requiring covered entities to ensure all devices accessing ePHI are configured, positioned, secured and used in a manner that protects from unauthorized disclosure of ePHI.

II. SCOPE

This policy and procedure document applies to all mobile devices, regardless of ownership, that access County Health Agency information resources regardless of form or media. Mobile devices include but are not limited to: PDA's smart phones, laptops, i-pads, tablets and kindles.

This policy and procedure document applies all employees, contractors, agents or volunteers of the San Luis Obispo County Health Agency conducting business on their personal mobile devices or County issued mobile devices.

III. POLICY

NOTE: This policy is an extension of the Workstation Security Policy, placing special emphasis on the unique security risks associated with the use of mobile devices.

Conduct of all Health Agency business using mobile devices shall at a minimum be consistent with the County IT Acceptable Use Policy and County Information Security Program Policies. In addition, the following policies apply:

A. Authorized Use

1. ePHI Access - Personal mobile devices used for access to ePHI must be approved and documented by the Security Officer prior to accessing the County Network. Such approval shall include verification of acceptable anti-virus software on the mobile device.
2. ePHI Storage - Only employees with authorization may store ePHI on mobile devices. Such authorization may be requested by the employee's supervisor and approved by the HIPAA Security Officer.

B. Network Access

1. Mobile devices that have not been approved by the Security Officer may not store ePHI and may not access the County network.
2. Access to the County network from a mobile device shall be via secure means and shall be consistent with procedures issued by the HIPAA Security Officer.
3. Employees shall access only that data to which they have authorization and have a need to know. No employee shall access or attempt to access data for which they do not have authorization.

C. Encryption / Password Protection

All mobile devices that access or store ePHI shall have encryption software as approved by the HIPAA Security Officer or shall have strong password protection as approved by the HIPAA Security Officer. No mobile device may access or store ePHI without such protection installed. SEE DHCS CONTRACT EXHIBIT F (Technical Controls).

D. Automatic Lockout / Logoff

1. All mobile devices with access to ePHI, regardless of ownership, shall be set to automatically “session-lock” after a period of inactivity. Such period shall not exceed 10 minutes with a recommended inactivity timeout of 5 minutes.

2. Employees shall manually lock their mobile device using Ctrl-Alt-Delete or similar locking procedure when idle.

3. Employees must maintain control of their mobile device at all times.

E. Device Positioning

Because of the mobile nature of mobile devices, employees must take extra care when viewing ePHI. Employees shall ensure that observable confidential information is adequately shielded from unauthorized disclosure and unauthorized access. Employees shall make every effort to ensure confidential information on computer screens is not visible to unauthorized persons.

F. Authorized Software

1. Employees shall not install software on mobile devices owned or operated by the Health Agency without prior approval by their immediate supervisor and the HIPAA Security Officer.

2. Health Agency IT shall monitor all logins to workstations and applications including failed logon attempts.

G. Data Storage on Mobile Devices

In cases where ePHI has been stored on a mobile device, it shall be fully deleted or removed as soon as the need for the data ends. Removal includes permanent deletion from electronic trash cans.

H. Reporting a Lost or Stolen Mobile Device

Members of the workforce must immediately report any mobile device that has been lost or stolen after being used to access or store County controlled PHI. The loss or theft must be reported to their supervisor, manager, department HIPAA Privacy Officer, or the department HIPAA Security Officer. HIPAA regulations require the County to report loss or theft of ePHI to the Department of Health Care Services within 24 hours. As such, immediate reporting is essential to meet this statutory timeline.

IV. APPLICABLE STANDARDS/REGULATIONS

- 45 CFR 164.310(b)-164.310(c) requires covered entities to implement policies and procedures specifying appropriate use of a workstation to ensure security of ePHI as well as standards for how the workstation shall be physically protected to ensure security of ePHI.

- 45 CFR 164.312(a)(2)(iii) requires covered entities to implement policies and procedures for logging off when workstation is unattended and for automatic locking after a period of inactivity.

Storage of Information on Removable Media Devices or Mobile Devices

(Security Policy and Procedure #10)

I. PURPOSE

This policy and procedure is intended to ensure compliance with HIPAA statutes and other regulations requiring covered entities to govern the receipt, use, movement, reuse and disposal of hardware and electronic media in a manner that protects ePHI.

II. SCOPE

This policy and procedure document applies to the privacy and security of all hardware and software used to access, store or transmit ePHI controlled by the County Health Agency regardless of form or media.

This policy and procedure document applies all employees, contractors, agents or volunteers of the San Luis Obispo County Health Agency.

III. POLICY

A. Authorized Use of Removable Storage Devices or Mobile Devices

1. No ePHI may be stored on removable storage or mobile devices without the written consent of the employee's supervisor and approval of the HIPAA Security Officer. Removable storage devices include but are not limited to: flash drives, external hard drives, DVDs and CDs. Mobile devices include but are not limited to: PDA's smart phones, laptops, tablets, kindles.

2. No ePHI may be stored in web-based storage or cloud based storage without the written consent of the employee's supervisor and approval of the HIPAA Security Officer.

3. All mobile devices storing ePHI must be registered with the HIPAA Security Officer. The HIPAA Security Officer shall maintain a log documenting the type of media device, the person using the device, and the reason for storing ePHI on a mobile device.

4. No ePHI on any type of storage device may be removed from County premises without written authorization of the employee's supervisor and approval by the HIPAA Security Officer.

B. General Security Conditions for Use of Removable Storage or Mobile Devices

1. No ePHI may be stored on personal removable data storage devices. All devices (flash drives, DVDs, CDs, etc.) storing ePHI must have been issued by the HIPAA Security Officer. The HIPAA Security Officer shall track and document the issuance of all such devices.

2. Any ePHI stored on removable storage or mobile devices must be backed up on a SLOCO network server no more than 24 hours after creation or receipt of such information. Transferring data from a removable storage or mobile device to the network server must be accomplished through secure methods as approved by the HIPAA Security Officer.

3. All removable media devices storing ePHI must be encrypted. Mobile devices storing ePHI shall have encryption software or strong password protection as approved by the HIPAA Security Officer.

4. Employees must secure and control removable media devices or mobile devices at all times. No removable media devices or mobile devices may be left visible in a vehicle or any other unsecure location.

C. Reuse of Hard Drives, Removable Storage, or Mobile Devices

1. All ePHI shall be removed from device hard drives, removable media devices, or mobile devices when the equipment is transferred to a worker who does not require access to the ePHI or when the equipment is transferred to a new worker with different ePHI access needs. Hard drives shall be wiped clean before transfer. Cleaning shall meet the Department of Defense (DOD) standards which states "the method of destruction shall preclude recognition or reconstruction of the classified information or material." In addition, the hard drive or device shall be tested to ensure the information cannot be retrieved.

2. All other media shall have all the ePHI removed (the mechanism may vary depending on the media type) and tested to ensure the ePHI cannot be retrieved. If the media is not "technology capable" of being cleaned, the media shall be overwritten or destroyed.

D. Disposal of Device Hard Drives, Removable Storage, or Mobile Devices.

Before electronic media that contains ePHI can be disposed, the following actions shall be taken on hard drives, removable storage, or mobile devices used to access or store ePHI or ePII.

1. Hard drives shall be either wiped clean or destroyed. Hard drive cleaning shall meet the Department of Defense (DOD) standards, which states "the method of destruction shall preclude recognition or reconstruction of the classified information or material." In addition, the hard drive shall be tested to ensure the information cannot be retrieved.

2. Backup tapes shall be destroyed or returned to the owner and their return documented. Destruction shall include a method to ensure there is no ability to reconstruct the data.

3. Other media such as memory sticks, USB flash drives or micro drives, CD-ROMs and floppy disks, shall be physically destroyed (broken into pieces) before disposing of the item.

E. Acquisition of Devices that Store ePHI

The Health Agency shall include security requirements and/or security specifications in information system acquisition contracts based on an assessment of risk (applications, servers, workstations, copiers, etc.)

F. Device Maintenance and Repair

All ePHI shall be removed from a device a device's memory or hard drive before the device is accessed for maintenance or sent out for repair. Devices include computer servers, copiers, printers, and other devices capable of storing ePHI. Copier hard drives shall be set to auto-erase daily.

G. Reporting a Lost or Stolen Removable Media Device

Any employees, contractors, agents or volunteers who have access to electronic health records through a mobile device must immediately report any removable media device that has been lost or stolen after being used to access or store County controlled PHI. The loss or theft must be reported to their supervisor, manager, department HIPAA Privacy Officer, or the department HIPAA Security Officer. HIPAA regulations require the County to report loss or theft of ePHI to the Department of Health Care Services within 24 hours. As such, immediate reporting is essential to meet this statutory timeline.

IV. APPLICABLE STANDARDS/REGULATIONS

- 45 CFR 164.310(d) requires covered entities to maintain policies and procedures to govern the receipt, movement, removal, reuse and disposal of hardware and electronic media that contain ePHI.

ePHI Data Transmission Security and Integrity

(Security Policy and Procedure #11)

I. PURPOSE

This policy and procedure is intended to ensure compliance with HIPAA statutes and other regulations requiring covered entities to ensure the security and integrity of ePHI while being transmitted electronically.

II. SCOPE

This policy and procedure document applies to the privacy and security of all ePHI controlled by the County Health Agency regardless of form or media.

This policy and procedure document applies all employees, contractors, agents or volunteers of the San Luis Obispo County Health Agency.

This Policy applies to all transmission of ePHI from covered components of the Health Agency. It includes e-phi transmitted to via e-mail, fax, or other electronic means of data transmission.

III. POLICY

A. All employees of the Health Agency shall take steps to ensure that transmission of ePHI will be secure and will be protected from unauthorized access or disclosure.

B. All transmission of ePHI shall include the Health Agency's standard confidentiality statement.

C. All transmission of e-PHI shall be limited to the minimum amount necessary to perform the intended task.

D. ePHI shall not be transmitted to a distribution list (Whether by fax, e-mail or other electronic means.)

E. All PHI transmitted via e-mail, *outside of the County Lotus Notes system,* shall be in encrypted form. (E-mails send within the county Lotus Notes system cannot be encrypted, therefore only the attachments must be encrypted.)

F. Any person who transmits PHI and/or PII electronically must understand and comply with the following:

1. County of San Luis Obispo Information Security Policies.
2. Applicable contract provisions (For example, your program may have a state contract that has additional restrictions on electronic transmission of information.)
3. HIPAA or other privacy-related policies & procedures or regulations specific to the unit of the Health Agency which creates, maintains, receives or transmits the PHI and/or PII.

G. Any employee, contractor or volunteer who is aware that ePHI may have been improperly disclosed is aware that this policy has been violated must report the violation to their supervisor, manager, department HIPAA Privacy Officer, or the department HIPAA Security Officer immediately. Improper disclosure includes but is not limited to: sending to a wrong e-mail, sending to a wrong fax, sending to an unintended recipient, including more than minimally necessary information, including improper personally identifying information.

NOTE: HIPAA regulations require the County to report select violations to the Department of Health Care Services within 24 hours. As such, immediate reporting is essential to meet this statutory timeline. The violation must be reported whether committed by the person reporting the violation, or another individual and it must be reported whether intentional or accidental.

H. Imaging of PHI or PII may only be done on a County owned photocopier. Imaging PHI or PII with a camera, camera phone, or any other imaging device is strictly prohibited.

IV. PROCEDURES AND STANDARDS

A. Encryption

1. Proven, standard algorithms shall be used as the basis for encryption technologies.
2. All ePHI sent via e-mail to an e-mail address outside the county e-mail system must be encrypted. (Note: E-mail sent *within* the county Lotus Notes e-mail network cannot be encrypted, however any *attachments* to e-mails sent *within* the Lotus Notes e-mail network must be encrypted. See additional policy below.)
3. When accessing the county network remotely, the county VPN network shall be used.

B. Transmission Using Wireless LAN and Devices

Transmission of ePHI over a wireless network is permitted under the following conditions:

1. The device is connected to the "Secure_WAN" provided by the County (County WiFi); or
2. The device is connected via County VPN when using a non-County provided wireless network.
3. All of the conditions in the policy section above, (Minimum necessary standard, Confidentiality statement, Encryption if necessary, etc.) are followed.

C. Perimeter Security

Any external connection to the Wide Area Network (WAN) must be authorized by the HIPAA Security Officer. Inbound services shall be negotiated on a case by case basis with the HIPAA Security Officer. All connections shall at a minimum comply with County IT security standards.

D. Firewall Controls

Networks containing systems and applications with ePHI shall implement perimeter security and access control with a firewall. Firewalls shall be configured to support the following minimum requirements:

1. Limit network access to only authorized employees and entities; Limit network access to only legitimate or established connections; and
2. Console and other management ports shall be appropriately secured or disabled.

E. General Safeguards and Guidelines on the Transmission of PHI via electronic means.

Employees are expected to utilize appropriate safeguards when transmitting or disclosing PHI. *These guidelines are not required for all transmission of PHI, however they are suggested practices that an employee should consider to minimize the risk of improper disclosure of PHI or PII.* Safeguards include but are not limited to:

1. Use the safest practical means to communicate PHI, which may not involve the electronic transmission of health care information. Examples include:
   a. Call or meet face-to-face with the intended recipient of the PHI.
   b. File electronic PHI in a protected folder on a shared drive and send a link to the intended recipient.
   c. Ask the intended recipient to review the PHI where it is safely stored in the Electronic Health Record.
2. De-identify the PHI prior to transmitting or forwarding electronically.
   a. PHI is health information that identifies the individual to whom it pertains. Once all PII is removed, de-identified health information may be safely transmitted electronically.
   b. Prior to sending or forwarding electronic communication, remove PII from:
      i The subject line and the body of emails
      ii The body and file name of all attachments
   c. How to safely identify a client in an electronic communication:
      i Preferred method:
         - *Include a client number that is used only by a system under the secure control of the Health Agency (for example, the Anasazi client number).*
      ii Acceptable methods if a client number is not available:
         - *Call the intended recipient(s) and advise them that you are sending an electronic communication to them. Identify the client by phone. DO NOT leave any PII on voicemail unless the identity of the recipient is confirmed AND the voicemail is accessible only to the intended recipient.*
         - *Reference the client's identity in such a way that only your recipient could understand (such as referring to an earlier conversation about the client).*
         - *Use only the client's initials, as long as those initials are not highly unusual or recognizable by others.*
   d. Examples of how to de-identify client health information
      i Examples *of* de-identified health care information:
         - "Referred client #555443 to specialist for chronic diabetes."

      (Only authorized Health Agency employees may access the system that cross references this client # with a name)
         - "Referred the client (initials JS), whom we discussed on the phone yesterday, to specialist for chronic diabetes."

      (Initials are common and will not likely identify the client to anyone other than the intended recipient)

      ii Examples of a failure to de-identify PHI:
         - "Referred Medi-Cal case# 123456789A to specialist for chronic diabetes."

      (Client may be identified by anyone with access to the statewide Medi-Cal Eligibility Data system (MEDS))
         - "Referred the client (initials ZZ), whom we discussed on the phone yesterday, to specialist for chronic diabetes."

      (Initials are unusual enough to potentially identify the client)
         - "Referred the tall, bearded Australian client to specialist for chronic diabetes."

      (Identifying clues are unusual enough to potentially identify the client)
         - "Our mutual client, John Smith, told me in session yesterday …."

      (Client names are <u>never</u> acceptable in the body of an email or in an unencrypted attachment).

3. Confirm the recipient before sending emails, faxes or other electronic communication.
    a. Verify the "to" field prior to sending the message to ensure positive identification of the person to whom you are sending the message.
    b. Do not rely on an auto-fill or auto-populate function to accurately address a communication. (Typical in e-mail and text messaging applications.)
        i Select the recipient from a pick list. When composing an email, click on the bolded word "To" and select the recipient from the list or select using the Contacts menu.
        ii Select each recipient separately. It is against this policy to send PHI using a group distribution list.
    c. Take reasonable steps to authenticate the identity of recipients before sending PHI. For example, you may want to send a test e-mail or fax and request confirmation prior to sending the e-mail with PHI.
    d. Confirm that the transmission includes the appropriate confidentiality statement on the facsimile cover sheet or email footer.
4. Obtain client consent prior to using electronic means to communicate with a client.
    a. Inform client of the risks and limitations associated with electronic communication, such as email or texting.
    b. Prior to any electronic communication, the client must complete and sign the Client Electronic Communication Consent form.
    c. The client must complete a separate consent form for each employee with whom he/she wishes to communicate via email or text. However, if the client sees multiple employees in a group setting he/she may sign one consent form covering the entire group.
    d. Maintain the consent form in the client's medical record and document additional communication preferences, special requests, and updates.
    e. Electronic transmission with clients should be limited to scheduling, routine follow-up, and other administrative communications. Do not transmit clinical information, such as test results, diagnostic or treatment information to clients. If a client initiates an email communication that includes clinical information, switch to a phone or in-person discussion.
    f. Emergency subject matter must not be sent to a client electronically.
    g. Copies of all messages pertinent to a client's care and treatment must be included in the client's medical record and are subject to electronic discovery.

F. Standards by Transmission Method

Electronic transmission of PHI may only be performed via encrypted e-mail, fax, voicemail or text messaging. No other electronic method is approved for transmitting PHI. A signed Client Electronic Communication Consent form is required prior to any communication of PHI using e-mail or text messaging.

1. E-mail Transmissions

   a. Only authorized County email accounts may be used to send or receive email with PHI. Do not forward, receive or send PHI to or from your personal email account.

   b. Client consent must be obtained prior to transmitting PHI via e-mail. See: Client Electronic Communication Consent

   c. PHI sent via electronic mail must be encrypted.
      i. Note: Sending e-mail from an encrypted computer does not encrypt the e-mail. Computer encryption simply protects the hard drive from improper access. E-mails must be individually encrypted to ensure protection during the transmission and receipt process.
      ii. PHI *must not* be included in the subject line of an e-mail because the subject line is generally not protected by encryption software.

   d. E-mail containing PHI sent *within* the County e-mail system.
      i. While the entire e-mail within the Lotus Notes system cannot be encrypted while sending between County e-mails, ***attachments*** containing PHI being sent ***inside*** of the county Lotus Notes system must be encrypted.
      ii. There are many "Zip and Encrypt" software solutions on the market. Please contact Health Agency IT if you do not know how to encrypt an e-mail attachment.

   e. E-mail containing PHI sent *outside of* the County e-mail system.
      i. E-mails containing PHI and PII (to a recipient not in the County email system) must be secured by the County's e-mail encryption tool. E-mail Encryption Instructions.

   f. PHI may only be sent to confirmed electronic mail addresses, and are not to be sent to distribution lists.

   g. Electronic mail may be used to communicate with patients, but it should not be used to respond to requests for copies of medical records. Specifically, complete medical record copies are not to be sent in electronic file form as attachments to an e-mail.

   h. In the absence of a system-generated confidentiality message, employees must ensure that electronic mail containing PHI includes the Health Agency's standard Confidentiality message.

1. Fax Transmissions

   a. ePHI shall only be faxed to confirmed fax numbers, and shall not be sent to distribution lists. For routine transmission of PHI via Fax, numbers should be programmed to minimize the potential for error. These numbers should be checked periodically to ensure they are correct

   b. All outgoing faxes containing PHI must include a separate cover sheet. Post-it notes are not an acceptable cover sheet. The Fax cover sheet shall minimally include the following information:

      i County Health Agency Seal or other appropriate logo
      ii Recipient name, fax, and phone number
      iii Sender name and phone number
      iv Subject (without identifying information), Date, Number of pages
      v Confidentiality statement

2. Voicemail Transmission

   a. Use of voice mail to communicate PHI is permitted only when the voice mailbox has a message specifically stating the name of the intended recipient and the sender is reasonably assured that the intended recipient is the only person with access to the voicemail box.

   b. Transmission of PHI via voicemail should be limited to information such as scheduling, routine follow-up, and other administrative communications, and should be de-identified to the extent possible.

3. Text Messaging

   a. Use of text messaging to transmit PHI may only be done with the consent of the client. See: Client Electronic Communication Consent.

   b. Special care must be taken when communicating PHI via text messaging. Text messaging is not encrypted and more vulnerable to improper disclosure than other electronic methods of transmission. Transmission of PHI via text messaging should be limited to information such as scheduling, routine follow-up, and other administrative communications, and should be de-identified to the extent possible.

V. APPLICABLE STANDARDS/REGULATIONS

- 45 CFR 164.312(e) requires covered entities to implement policies, procedures and technical safeguards in place to ensure the security and integrity of ePHI while being transmitted electronically.

Protection from Malicious Software

(Security Policy and Procedure #12)

I. PURPOSE

This policy and procedure is intended to ensure compliance with HIPAA statutes and other regulations requiring covered entities to protect systems that store and manage ePHI against malicious software, malware, viruses and other electronic system threats.

II. SCOPE

This policy and procedure document applies to the privacy and security of all ePHI controlled by the County Health Agency regardless of form or media.

This policy and procedure document applies all employees, contractors, agents or volunteers of the San Luis Obispo County Health Agency.

III. POLICY

A. The Health Agency shall ensure all computers (owned, leased, and/or operated by the covered components) install and maintain anti-virus software. All workstations shall be configured to activate and update anti-virus software automatically.

B. In the event that a virus, worm, or other malicious code has infected or been identified on a server or workstation, that equipment shall be disconnected from the network until it has been appropriately cleaned.

C. Employees shall only install software that has been approved by their supervisor and the HIPAA Security Officer on computers owned or operated by the Health Agency.

D. Devices using software or operating systems that are no longer supported by the originating vendor or applications for which the vendor will not allow patching of vulnerabilities (e.g., because it will cause proprietary or legacy applications to fail) shall be individually documented may only be connected to the County network with approval of the HIPAA Security Officer.

E. Business Associate and third-party owned devices may use their own standard anti-malware software, but must comply with National Institute of Standards and Technology (NIST) standards and the intent of this policy.

IV. PROCEDURE

Periodically, all workstations and mobile devices within the County Health Agency will be inspected either electronically or manually to ensure that:

A. An acceptable suite of anti-malware software is installed and running properly.

B. The anti-malware engines and signatures in use are the most current available.

C. All required patches, fixes, service-packs etc. for the operating system and installed applications have been installed.

D. “Session-lock” controls are set to Health Agency standards.

V. APPLICABLE STANDARDS/REGULATIONS

- 45 CFR 164.308(a)(5)(ii)(B) requires covered entities to implement effective security measures that protect against malicious software, malware, viruses and other electronic system threats.

Continuity of Service and Contingency Plan

(Security Policy and Procedure #13)

I. PURPOSE

This policy and procedure is intended to ensure compliance with HIPAA statutes and other regulations requiring covered entities to implement effective strategies and technologies for recovering access to ePHI in the case of disruption of access due to natural or man-made incident, emergency or disaster.

II. SCOPE

This policy and procedure document applies to the privacy and security of all ePHI controlled by the County Health Agency regardless of form or media.

This policy and procedure document applies all employees, contractors, agents or volunteers of the San Luis Obispo County Health Agency.

III. POLICY

A. The County shall maintain a Continuity of Service Plan to protect ePHI from damage, loss, or lack of availability and ensure continuity of service in the event of a natural or man-made incident, emergency or disaster. In compliance with HIPAA statutes, such plan shall contain the following elements:

1. Data Backup Plan
2. Disaster Recovery Plan
3. Emergency Mode Operation Plan
4. Testing and revision Procedures
5. Application and Data Criticality Analysis

B. All ePHI must be stored or replicated on a secure network server as identified and maintained by the HIPAA Security Officer.

C. The HIPAA Security Officer shall conduct periodic training and simulation drills on continuity of access to ePHI to ensure readiness.

IV. PROCEDURE

A. Place the procedure into Health Agency COOP Document Exhibit L

B. Also reference 4.2.6 of the COOP

V. APPLICABLE STANDARDS/REGULATIONS

- 45 CFR 164.308(a)(7) requires covered entities to implement effective strategies and technologies for recovering access to ePHI in the case of disruption of access due to natural or man-made incident, emergency or disaster.

Facility Access Controls

(Security Policy and Procedure #14)

I. PURPOSE

This policy and procedure is intended to ensure compliance with HIPAA statutes and other regulations requiring covered entities to protect the facilities housing ePHI and equipment therein from unauthorized access, tampering, and theft.

II. SCOPE

This policy and procedure document applies to all facilities controlled by the County Health Agency and housing equipment that stores or accesses ePHI..

This policy and procedure document applies all employees, agents or volunteers of the San Luis Obispo County Health Agency.

III. POLICY

A. SLOHA shall, to the extent reasonable in a public healthcare provider setting, implement physical safeguards and controls intended to secure facilities where ePHI is accessed.

B. SLOHA maintains security measures to safeguard and secure facilities where ePHI is stored.

IV. PROCEDURE

A. Facility Access

1. To the extent reasonable in a public healthcare provider setting, public entrances to Health Agency facilities providing services to the public shall be limited to the number necessary to provide effective service.

2. All keys and fobs issued to Health Agency employees shall be documented.

3. Facilities storing ePHI shall maintain physical security of hardware all times.

B. Access Management

1. Issuance and return of keys and fobs.

The Health Agency Personnel function shall issue and receive keys and fobs. The issuance and receipt of keys and fobs shall be documented.

2. Employee separation from Health Agency

Supervisors are responsible for recovering the key and/or fob from any employees who separates from the Health Agency. The key or fob must be returned to the Health Agency personnel function and recorded. Failure to recover by a separated employee shall be reported to Health Agency management.

3. Lost key and/or fob

Any employee who has lost or misplaced a key or fob must report the loss to their supervisor within one (1) working day. The Supervisor shall report the lost key to the Health Agency personnel function who will report the loss to Health Agency Management. All lost keys and/or fobs shall be documented in the Facility Security Log.

4. Health Agency Management shall assess the risk of a lost key or fob and shall determine whether re-keying shall be necessary. If rekeying is necessary, it shall be logged in the Facility Security Log.

C. Facility Security Standards for Employees.

1. Do not share keys or fobs that access a SLOHA facility or office containing ePHI.
2. Do not allow other persons to enter the facility by “piggy backing” (entering the facility by walking behind an authorized person through a door without using a key or fob) through a secure entrance unless you know the individual has authorized access.
3. When using secure doors, always ensure they are completely shut before leaving the door. Do not prop open doors intended to be locked and secure. It is the responsibility of an employee who is aware of a door that has problems with locking or automatically latching to report the problem to management.
4. Immediately report individuals who are believed to be in an area of the facility without authorization or without a business need to be in that area of the facility.

V. APPLICABLE STANDARDS/REGULATIONS

- 45 CFR 164.308(a)(2)(ii)- 164.308(a)(2)(iv) requires covered entities to implement effective policies that protect the facilities and equipment therein from unauthorized physical access, tampering, and theft.

Audit Controls and Data Integrity

(Security Policy and Procedure #15)

I. PURPOSE

This policy and procedure is intended to ensure compliance with HIPAA statutes and other regulations requiring covered entities to implement hardware, software, and/or procedural mechanisms that record and examine activity in systems that store or access ePHI.

II. SCOPE

This policy and procedure document applies to systems and procedures designed to protect ePHI.

III. POLICY

A. The Health Agency shall, conduct audits necessary to comply with HIPAA statutes and other regulations that require procedures and data be audited for the purpose of securing the privacy and integrity of ePHI.

B. The HIPAA Security Officer shall maintain matrix of audits to be conducted and shall maintain documentation of the result of audits performed.

IV. APPLICABLE STANDARDS/REGULATIONS

- 45 CFR 164.312(b) requires covered entities to implement hardware, software, and/or procedural mechanisms that record and examine activity in systems that store or access ePHI.
- 45 CFR 164.312(b) requires covered entities to implement policies and procedures to protect ePHI from improper alteration or destruction.

San Luis Obispo County Health Agency

Health Information Privacy and Security Policy and Procedure Suite

Chapter 3
General Provisions, Policies & Procedures

Incident Response and Incident Reporting

(Security Policy and Procedure #4)

I. POLICY

Any known incidents that are related to or affect the privacy, confidentiality or integrity of ePHI or other PHI shall be identified, reported, and documented. In addition, the Health Agency shall identify any harmful effects of a security issue and mitigate those harmful effects to the extent practicable. Reporting responsibility is as follows:

A. Employee, Contractor, Agent or Volunteer Reporting

An employee, agent or volunteer of the Health Agency who has a reasonable belief that the County's HIPAA privacy or security policies and procedures have been violated must report the violation to their supervisor, manager, department HIPAA Privacy Officer, or the department HIPAA Security Officer immediately. Regulations require the County to report select violations to the Department of Health Care Services within 24 hours. As such, immediate reporting is essential to meet this statutory timeline. The violation must be reported whether committed by the person reporting the violation, or another individual and it must be reported whether intentional or accidental.

B. Supervisor and Manager Reporting

A supervisor or Manager who is made aware of a security incident, threat or vulnerability under this policy shall report the incident to a designated HIPAA Privacy Officer or the HIPAA Security Officer.

C. All reports of a HIPAA related incident involving ePHI must be logged by the HIPAA Security Officer on the HIPAA Incident Log.

D. Additional Contacts

Employees may also contact the following if they are aware of or suspect violation of these policies or applicable regulations:

- You can call the toll-free confidential hotline at: **(855) 326-9623**
- Or you can contact us by e-mail at: privacy@co.slo.ca.us
- Or send a letter to:
  Privacy Officer
  San Luis Obispo County Health Agency
  2180 Johnson Avenue
  San Luis Obispo, CA 93401

You may also contact the Department of Health and Human Services at:

Office of Civil Rights
90 7th Street, Suite 4-100
San Francisco, CA 94103

- Or you can file a complaint online at: www.hhs.gov/ocr/privacy/hipaa/complaints
- Or call toll free at: (800) 368-1019 - TDD (800) 537-7697

II. PROCEDURE

A. Incident or Threat Assessment

Upon receiving a report of a security incident or threat, the HIPAA Privacy Officer or HIPAA Security Officer shall assess the nature of the incident using the Health Agency Incident Assessment and Mitigation Report. The Officer may seek advice further advice from the Health Agency Director or designee, County Information Technology, County Counsel, or may seek to convene the Health Agency Compliance Steering Committee.

B. Response and Mitigation

1. If the matter can easily be corrected and mitigated, the Officer completing the report will take necessary steps to correct the incident and will document the steps taken on the Breach Risk Assessment Form. A copy of the final report shall be provided to the HIPAA Security Officer.
2. If the reported incident requires resources, expertise or authority beyond that of the HIPAA Privacy Officer or HIPAA Security Officer, the Officer may seek advice further advice from the Health Agency Director or designee, County Information Technology Department, County Counsel, or may seek to convene the Health Agency Compliance Steering Committee. Mitigating measures will be assessed and implemented where appropriate and consistent with statute. A copy of the final Health Agency Incident Assessment and Mitigation report shall be provided to the HIPAA Security Officer.

C. Incident Logging

All reports of a security incident or threat shall be logged on the HIPAA Incident Log. All incident reports shall be supported by a completed Breach Risk Assessment Form.

III. APPLICABLE STANDARDS/REGULATIONS

- 45 CFR 164.308(a)(6) requires that covered entities respond to and document suspected or known security incidents and mitigate harmful effects to the extent practicable.
- AB 1149 amending Section 1798.29 of the California Civil Code.

IV. RESOURCES

A. Incident Report Form (For Employee Use)
B. Breach Risk Assessment Form
C. DHCS Privacy Incident Report Form
D. Health Agency Incident Assessment and Mitigation Report
E. HIPAA Incident Log

Breach Reporting Policy

II. PURPOSE

Various statutes, regulations, and contractual agreements limit the acquisition, access, use and disclosure of Protected Health Information (PHI) and Personally Identifiable Information (PII). These laws and agreements include but are not limited to:

A. Health Information Technology for Economic and Clinical Health Act (HITECH Act)

B. HIPAA Privacy Rule, 45 C.F.R 164.500 et seq.

C. Contract between San Luis Obispo County and the State Department of Health Care Services

D. State of California - AB 211, SB541

E. Title XIII of Division A of the American Reinvestment and Recovery Act of 2009 (ARRA)

F. Regulations from Interim Rule pub. August 24, 2009 in Federal Register (74 Fed. Reg. 42740)

G. California Civil Code 1798 (Personally Identifiable Information).

These laws further require the reporting of any acquisition, access, use or disclosure that is not specifically permitted. This document complies with requirements to establish policies and procedures for reporting non permitted disclosures of PHI and PII.

III. POLICY

1. Any employee, volunteer, student, agent, contractor, business associate or other person or entity who knows or suspects that there has been a breach of PHI or PII shall immediately notify a supervisor, manager, HIPAA Privacy Officer, or HIPAA Security Officer of the breach or suspected breach. Regulations require the County to report breaches to some state agencies within 24 hours. As such, immediate reporting is essential to meet this statutory timeline. The breach must be reported whether committed by the person reporting the violation, or another individual and it must be reported whether intentional or accidental.

NOTE: A breach may be reported to any employee by a client or other member of the public. It is the responsibility of the person receiving the initial report to obtain as much information about the breach as reasonable without violating the person's privacy. Contact information for the person is the most important to obtain; however dates of the breach, names of employees potentially involved in the breach, Department in which the potential breach occurred, and a summary of the breach will be helpful in starting an investigation.
Employees who have reported a breach to a supervisor, manager, HIPAA Privacy Officer, or HIPAA Security Officer shall not discuss the breach or suspected breach with other employees unless directed to do so.

2. Any supervisor or manager who has received a report of a breach or suspected breach shall immediately notify a HIPAA Privacy Officer or HIPAA Security Officer.
3. The person reporting the breach must follow up the report with documentation on an Incident Report Form (Public Health) or a Behavioral Health Incident Report Form and shall submit it to the supervisor or manager to whom the breach was reported.
4. The person receiving the report of the breach shall follow the procedures for investigating the breach and determining appropriate response and mitigation measures if necessary.

NOTE: Any non-permitted disclosure of PHI is presumed to be a breach unless the County demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment as described in HIPAA regulations.

II. PROCEDURE

A report of a breach or suspected breach may be made via any of the following:

A. PHONE - Call any HIPAA Privacy Officer by leaving a message at (805) 781-4788. The all of the HIPAA Privacy team will be notified by e-mail that a message has been left. Please be sure to leave your name, position, department and contact information.

1. E-MAIL - Send an e-mail to: HA_Compliance. Please be sure to include your name, position, department and contact information.

2. IN PERSON – See any supervisor, manager, HIPAA Privacy Officer, or Department Head to report the breach or suspected breach.

III. APPLICABLE STANDARDS/REGULATIONS

A. Health Information Technology for Economic and Clinical Health Act (HITECH Act)
B. HIPAA Privacy Rule, 45 C.F.R 164.500 et seq.
C. Contract between San Luis Obispo County and the State Department of Health Care Services
D. State of California - AB 211, SB541
E. Title XIII of Division A of the American Reinvestment and Recovery Act of 2009 (ARRA)
F. Regulations from Interim Rule pub. August 24, 2009 in Federal Register (74 Fed. Reg. 42740)
G. California Civil Code 1798 (Personally Identifiable Information).

Breach Investigation Policy and Procedure

I. PURPOSE

This policy and procedure document provides guidance to supervisors, managers, HIPAA Privacy Officers, and the HIPAA Security Officer regarding steps to be taken when a breach or suspected breach has been reported.

IV. SCOPE

This policy and procedure document applies to the privacy and security of all PHI and PII controlled by the County Health Agency regardless of form or media.

This policy and procedure document applies all supervisors and managers of the San Luis Obispo County Health Agency.

V. POLICY

A. Any supervisor or manager who has received a report of a breach or suspected breach shall immediately notify a HIPAA Privacy Officer or HIPAA Security Officer.

1. Depending on the nature of the breach and the program in which the breach occurred, the appropriate HIPAA Privacy Officer or the HIPAA Security Officer shall perform an initial assessment to determine whether a breach or attempted breach occurred. If it is determined that a breach occurred, the Officer investigating the matter shall at a minimum notify the appropriate Department Head, the Compliance Program Manager and the HIPAA Security Officer.

2. If the Officer investigating the matter determines that the matter should be reported to the Department of Health Care Services, the Federal Trade Commission, the State Attorney General, or other regulatory agency, the Officer shall submit the report in the appropriate format and on the prescribed forms.

3. The Officer reporting the matter shall follow the investigation procedure described below and at a minimum report the final findings to the appropriate Department Head, the Program Compliance Manager, and the Health Agency Director.

4. All documentation generated in the investigation of a breach must be retained for a period of six years.

VI. PROCEDURE

A. The investigating Officer must ensure that the employee who reported the breach or suspected breach submits a completed Incident Report Form (Public Health) or a Behavioral Health Incident Report Form.

1. The investigating Officer must take steps to examine evidence and interview witnesses in an effort to determine whether a breach in fact occurred. If the Officer determines that a breach occurred, they shall continue the investigation to determine the nature, scope and severity of the breach. Prior to interviewing employees who may have caused the breach or may be subject to discipline as a result of the breach, the Health Agency Human Resources Manager shall be consulted. Guidance for conducting an investigation can be found in the County Internal Investigation Guidelines (2005).

2. The Health Agency Breach Risk Assessment Form shall be used when investigating a breach.

3. After reviewing evidence including witness and subject interview statements, the investigating Officer shall write a report indicating:
   a. Facts describing the breach including the nature, scope and severity of the breach;
   b. Who was involved in the breach and their role;
   c. Measures recommended (if any) for mitigation of damages;
   d. Measures recommended to reduce the likelihood of similar breach;
   e. Reports (if any) made to regulatory agencies.

4. The investigator will provide copies of the final report to the Department Head, the Compliance Program Manager, and the Health Agency Director.

VII. APPLICABLE STANDARDS/REGULATIONS

A. Health Information Technology for Economic and Clinical Health Act (HITECH Act)
B. HIPAA Privacy Rule, 45 C.F.R 164.500 et seq.
C. Contract between San Luis Obispo County and the State Department of Health Care Services
D. State of California - AB 211, SB541
E. Title XIII of Division A of the American Reinvestment and Recovery Act of 2009 (ARRA)
F. Regulations from Interim Rule pub. August 24, 2009 in Federal Register (74 Fed. Reg. 42740)
G. California Civil Code 1798 (Personally Identifiable Information).

VIII. RESOURCES

A. Incident Report Form
B. Behavioral Health Incident Report Form
C. Health Agency Breach Risk Assessment Form
D. County Internal Investigation Guidelines (Apr. 2005)

Sanctions for Violation of Policy/Procedure

(Security Policy and Procedure #3)

I. PURPOSE

This policy and procedure is intended to ensure compliance with HIPAA statutes and other regulations that require sanctions to be considered against employees who fail to comply with the security policies and procedures contained herein.

II. SCOPE

This policy and procedure document applies to the privacy and security of all ePHI controlled by the County Health Agency regardless of form or media.
This policy and procedure document applies all employees, contractors, agents or volunteers of the San Luis Obispo County Health Agency.

III. POLICY

A. Disciplinary Actions and Sanctions

An employee of the Health Agency who violates any provision of the County's HIPAA privacy or security policies and procedures shall be subject to disciplinary actions up to and including termination of employment. An agent, volunteer or contractor of the County Health Agency who violates any provision of the Health Agency's HIPAA privacy or security policies and procedures shall be subject to sanctions which may include but are not limited to contract cancellation or termination of services.

1. Obligation to Report Violations

An employee, agent or volunteer of the Health Agency who has a reasonable belief that the County's HIPAA privacy or security policies and procedures have been violated must report the violation to their supervisor, manager, department HIPAA Privacy Officer, or the department HIPAA Security Officer immediately. HIPAA regulations require the County to report select violations to the Department of Health Care Services within 24 hours. As such, immediate reporting is essential to meet this statutory timeline. The violation must be reported whether committed by the person reporting the violation, or another individual and it must be reported whether intentional or accidental.

2. Prohibition Against Retaliation

Retaliation against any person who in good faith reports a violation of the Health Agency's HIPAA privacy or security policies and procedures or retaliation against any person who supports someone else who reports a violation of the policy is prohibited. In addition, retaliation against any person who cooperates in an investigation related to this policy is prohibited.

IV. APPLICABLE STANDARDS/REGULATIONS

- 45 CFR 164.308(a)(1)(ii)(C) requires that covered entities apply sanctions against employees who fail to comply with the security policies and procedures contained herein.

POLICY / HIPAA REGULATION CROSS REFERENCE

HIPAA Security Rule	HIPAA Section #	Policy #
Security Management Process	164.308(a)(1)	1 – 3
Risk Analysis		2
Risk Management		2
Sanction Policy	164.308(a)(1)(ii)(C)	3
Information System Activity Review		1
Assigned Security Responsibility	164.308(a)(2)	1
Workforce Security	164.308(a)(3)	8
Authorization and/or Supervision		8
Workforce Clearance Procedure		8
Termination Procedures		8
Information Access Management	164.308(a)(4)	8
Isolating Health Care Clearinghouse functions	164.308(a)(4)(ii)(A)	N/A no Clearing house
Access Authorization	164.308(a)(4)(ii)(B)	8
Access Establishment and Modification	164.308(a)(4)(ii)(C)	8
Security Awareness & Training	164.308(a)(5)(i)	7
Security Reminders	164.308(a)(5)(ii)(A)	7
Protection from Malicious Software	164.308(a)(5)(ii)(B)	12
Log-in Monitoring		7
Password Management		7
Security Incident Procedures	164.380(a)(6)	4
Response and Reporting		4
Contingency Plan	164.308(a)(7)	13
Data Backup Plan		13
Disaster Recovery Plan		13
Emergency Mode Operation Plan		13
Testing and Revision Procedure		13
Applications and Data Criticality Analysis		13
Evaluation	164.308(a)(8)	2
Business Associate Contracts	164.308(b)	5

Written Contract or Other Arrangements		5
Facility Access Controls	164.310(a)(1)	14
Contingency Operations		14
Facility Security Plan		14
Access Control and Validation		14
Procedures Maintenance Records		14
Workstation Use	164.310(b)	8 - 9
Workstation Security	164.310(c)	8 - 9
Device and Media Controls	164.310(d)(1)	10
Disposal	164.310(d)(2)(i)	10
Media Re-use	164.310(d)(2)(ii)	10
Accountability	164.310(d)(2)(iii)	10
Data Backup and Storage	164.310(d)(2)(iv)	13
Access Control	164.312(a)(1)	7
Unique User Identification		7
Emergency Access Procedure		7
Automatic Logoff	164.312(a)(2)(iii)	8 - 9
Encryption and Decryption		8
Audit Controls	164.312(b)	15
Integrity	164.312(c)(1)	15
Mechanism to Authenticate ePHI		15
Person or Entity Authentication	164.312(d)	7
Transmission Security	164.312(e)(1)	11
Integrity Controls		11
Encryption		11
Policies and Procedures	164.316(a)	1
Documentation	164.316(b)(1)	1

Definitions	
Terms	**Definitions**
Authorization	The formal consent document, signed by a client or their legal representative, authorizing the release of PHI from the records of an entity covered by the privacy provisions of HIPAA or other related regulations.
Business Associate	On behalf of one of the covered components, completes a function or activity involving the use or disclosure of protected health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, and practice management; or, provides, other than in the capacity of a member of the workforce of a covered entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a covered entity, where the provision of the service involves the disclosure of individually identifiable health information from the covered entity or arrangement, or from another business associate of a covered entity or arrangement, to the person.
Client	For the purposes of this policy and other policies related to protected health information, a client is defined as any individual who requests or receives services from SLOHA. Such services may be for an individual's physical health, behavioral health, or to provide assistance through a health plan.
Covered Component	Covered components are those departments in the County that must comply with the HIPAA Security Rule. The County's covered components include the Health Agency with the exception of Animal Services, Environmental Health Services, and Public Guardian; Auditor Controller Payroll Division; and Probation Drug Testing Function.
Custodian of Records	An employee or group of employees, designated by the Health Agency Director in writing, to make disclosures of Protected Health Information that are not authorized to be performed by any other employee.
Designated Records Set	A group of records maintained by or for a covered entity that: 1) Are the medical records and billing records about individuals maintained for or by a covered health care provider; 2) Are the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or 3) Are used, in whole or in part by or for the covered entity to make decisions about individuals. 4) For purposes of this definition, the term record means any item, collection or grouping of information that includes PHI and is maintained, used, collected or disseminated by or for a covered entity.
Device	A device is a unit of computing hardware, outside or inside the case or housing for the operating computer. A device is capable of providing input to the essential computer, receiving output, or both.
Disclosure	The release, transfer, provision of access to, or divulging in any other manner of PHI to persons not employed by or working within the County, or to persons employed by or working within the County who are not performing or assisting with a covered function of the County.

Terms	Definitions
Disposal	The removal or destruction of electronic protected health information from electronic media
Electronic Protected Health Information (ePHI)	Protected Health Information that is created, stored and/or transmitted in electronic systems or electronic devices. Such systems/devices include but are not limited to: electronic health information applications, internet, intranet, extranet, email, USB drives, computer hard drives, laptop computers, tablets, smart phones, magnetic tapes, floppy disks, CDs, optical devices.
Employee	For the purpose of this policy and other policies regarding protected health information, the term "employee" shall have the same general meaning as the term workforce as described in 45CFR 160.103. Specifically, employee shall include any employee, intern, trainee, contractor, volunteer, or other person whose conduct, in the performance of work for the County, is under the control of the County.
Encryption	A method of scrambling or encoding data to prevent unauthorized workforce members from reading or tampering with the data. Only individuals with access to a password or key can decrypt and use the data.
Facility	County owned or leased building in which workers access Electronic Protected Health Information (EPHI)
Firewalls	Special computer programs and hardware that are set up on a network to prevent intruder from stealing or destroying data
Hard Drive	A data storage medium that houses all of the electronic information and software programs on a computer. It is one of the most important pieces of hardware inside a computer.
Healthcare Operations	Healthcare operations include but are not limited to: • Clinical improvement; • Professional peer review; • Business management; • Accreditation and licensing; • Enrollment; • Underwriting; • Reinsurance; • Compliance; • Auditing; and • Rating.
Local Drive	In context to this policy, it is a computer's hard drive (not the network)
Malicious Software	A type of software that includes ways of attacking data integrity, the system itself or the confidentiality of the data. Malicious software includes viruses, virus variants, worms hoaxes, and trojan horses
Media Reuse	The reuse of a device such as a computer hard drive that contained data and that is being prepared for reuse with new data
Modem	A device that translates telephone tones to allow for the multiplexing of data information on the telephone network
Network	A group of computers and associated peripherals connected by a communications channel capable of sharing electronic information

Terms	Definitions
Network Closets	Concentration of network equipment such as hubs, routers, switches, racks, cables, and sometimes has telephone equipment
Payment	Includes the various activities of health care providers to obtain payment or be reimbursed for their services and of a health plan to fulfill their coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care. Examples include: • Determining eligibility or coverage under a plan and adjudicating claims; • Risk adjustments; • Billing and collection activities; • Reviewing health care services for medical necessity, coverage, justification of charges, and the like; and • Utilization review activities
Personally Identifiable Information (PII)	Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.
Protected Health Information (PHI)	PHI is individually identifiable health information held or transmitted by a covered entity or its business associate in any form or medium, whether electronic, on paper, or oral. PHI is information, including demographic information, which relates to: • The individual's past, present, or future physical or mental health or condition; • The provision of health care to the individual; • The past, present, or future payment for the provision of health care to the individual; And: • Identifies the individual or can reasonably be used to identify the individual ▪ The 18 identifiers that make health information PHI are: 1. Names; 2. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code; 3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89; 4. Phone numbers; 5. Fax numbers; 6. Electronic mail addresses; 7. Social Security numbers; 8. Medical record numbers; 9. Health plan beneficiary numbers; 10. Account numbers; 11. Certificate/license numbers; 12. Vehicle identifiers and serial numbers, including license plate numbers; 13. Device identifiers and serial numbers; 14. Web Universal Resource Locators (URLs); 15. Internet Protocol (IP) address numbers; 16. Biometric identifiers, including finger and voice prints; 17. Full face photographic images and any comparable images; and 18. Any other unique identifying number, characteristic, or code.

Terms	Definitions
Removable Media	Usually small devices carried or moved with ease that can contain electronic protected health information such as CD Rom Disks, laptops, USB drives
Risk Assessment	A process of assessing those factors that could affect confidentiality, availability, and integrity of key information assets and systems. Risk Assessment Authorities are responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets, while minimizing the impact of security procedures and policies upon business productivity.
Security Incident	Any condition that may threaten the privacy, security or integrity of ePHI, or may threaten the systems and processes intended to protect ePHI. These include but are not limited to: ▪ Virus, worm, or other malicious code attacks ▪ Network or system intrusions ▪ Persistent intrusion attempts from a particular entity ▪ Unauthorized access to ePHI, an ePHI based system, or an ePHI based network ▪ ePHI data loss due to disaster, failure, error, theft ▪ Loss of any electronic media that contains ePHI ▪ Loss of the integrity of ePHI ▪ Unauthorized person found in a covered component's facility
Server Room	The room where all the server computers are housed
Strong Passwords	A password that is difficult to detect by both humans and computer programs, effectively protecting data from unauthorized access. A strong password consists of at least six characters that are a combination of letters, numbers and symbols (@, #, $, %, etc.) if allowed. Strong passwords contain the maximum number of characters allowed. Passwords are typically case-sensitive so a strong password contains letters in both uppercase and lowercase. Strong passwords also do not contain words that can be found in a dictionary or any part of the user's own name.
Transmitting	The act of sending a message or data using an electronic medium.
Treatment	The provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another.
USB drives or USB flash drives	A small, portable flash memory card that plugs into a computer's USB port and functions as a portable hard drive with up to 2GB of storage capacity. USB flash drives are considered easy to use as they are small enough to be carried in a pocket and can plug into any computer with a USB drive.
Use	The application, utilization, examination, or analysis of protected health information within SLOHA, its affiliates, or its contract providers.

Terms	Definitions
User	For the purposes of this document, the term user refers to any workforce member (permanent or temporary), contractor, consultant, vendor, volunteer, student or other person who uses, maintains, manages or is otherwise given access privileges to County IT systems.
User ID	An identification code which identifies the user to County IT systems
Virtual Private Network (VPN)	A secure, private network connection between two or more devices across the public internet or other shared core network infrastructure. It allows computers at different locations to communicate with each other in a safe and secure environment.
Virus	A program that copies itself into another program, sectors on a drive, or into items that support scripts. Most viruses only copy themselves, while a minority unleash a payload, which is the action generated by the virus. Payloads can damage files, corrupt hard drives, display messages, or open other files. Typically, the payload is delivered when a certain condition occurs, such as when the date on the computer reaches a particular day.
Workforce member	In the HIPAA Privacy Rule, the term "workforce member" is defined as "employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.
Workstation	A networked computer that uses server resources, a computer that is connected to a mainframe computer. It is usually a personal computer connected to a Local Area Network (LAN), which shares the resources of one or more large computers. They can have their own applications installed, as well as their own hard disks.

County Health Agency Director Name: Jeff Hamm	Date: February 5, 2015 Signature: 
County Health Officer Name: Penny Borenstein, M.D.	Date: February 5, 2015 Signature: 
County Behavioral Health Administrator Name: Anne Robin	Date: February 5, 2015 Signature: