



City and County of San Francisco

Edwin M. Lee, Mayor

San Francisco Department of Public Health

Barbara A. Garcia, MPA
Director of Health

San Francisco Department of Public Health

Policy & Procedure Detail*

Policy & Procedure Title: DPH Privacy Policy	
Category: Privacy	
Effective Date: Adopted 3/2003, Revised 4/2006	Last Reissue/Revision Date: 9/23/2013
DPH Unit of Origin: SF DPH Privacy Office	
Policy Contact - Employee Name and Title; and/or DPH Division: Alice Gleghorn, Ph.D., SFDPH Privacy Officer	
Contact Phone Number(s): 415-255-3722	
Distribution: DPH-wide X	If not DPH-wide, other distribution:

**All sections in table required.*

1. Purpose of Policy

The purpose of this policy is to provide guidance to providers and other San Francisco Department of Public Health ("DPH") employees by setting forth the basic requirements for protecting the confidentiality of medical information as required by the Privacy Rule.

2. Policy

STATEMENT OF POLICY

It is the policy of the San Francisco Department of Public Health ("DPH") to comply with the Privacy Rule set forth in the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Each division and unit shall ensure that its policies and procedures are consistent with this department-wide policy and procedure.

SCOPE

This policy pertains to all individuals in the DPH who may access, use, or disclose protected health information, regardless of DPH division or unit. The policy is administered by the DPH Compliance Office through the activities of the DPH Privacy Officer. It is intended to serve as a foundation for privacy practices of the DPH. Divisions or units may impose privacy safeguards in addition to those required by this policy and procedure.

The mission of the San Francisco Department of Public Health is to protect and promote the health of all San Franciscans.

We shall ~ Assess and research the health of the community ~ Develop and enforce health policy ~ Prevent disease and injury ~
~ Educate the public and train health care providers ~ Provide quality, comprehensive, culturally-proficient health services ~ Ensure equal access to all ~

3. Definitions

BACKGROUND

The federal *Health Insurance Portability and Accountability Act of 1996* (HIPAA) established through its Administrative Simplification regulations to ensure privacy for individuals receiving health care services in the United States. The Privacy Rule, as it may also be called, establishes a national standard for the minimum level of protection for medical information. The intent of the statute and the regulatory rule is to expand consumer control over their medical information.

The Privacy Rule introduces the term "Protected Health Information," or "PHI." PHI covers information relating to an individual's health, the care received, and/or payment for services, including demographic data. It includes all information in any media related to the individual's health care that can be individually identified as belonging to a particular person.

The basic tenet of the Privacy Rule is that providers may use and disclose PHI without the individual's authorization only for treatment, payment, and health care operations, as well as certain public interest related purposes such as public health reporting. Other uses and disclosures of PHI generally require the written authorization of the individual.

The Privacy Rule also introduces the concept of "minimum necessary." This requirement mandates that when using or disclosing PHI, or when requesting PHI from external providers or entities, providers will make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose. The Privacy Rule does recognize that providers may need to use all of an individual's health information in the provision of patient care and/or public health purposes. However, access to PHI by the workforce must be limited based on job scope and the need for the information.

The Privacy Rule also includes a set of rights for consumers of health care services. These include the right to obtain a written notice explaining how DPH will use and disclose their information, to access their health information (including requesting copies, requesting amendments, and receiving an accounting of specified disclosures), to request that certain information be restricted from use or disclosure for purposes of treatment, payment and health care operations (this request need not be granted if it is unreasonable or overly burdensome), to request that information be communicated in particular ways to ensure confidentiality, and to refuse to authorize the release of information for most purposes not related to treatment, payment or health care operations.

This policy provides an overview of the requirements of the Privacy Rule. There are more detailed policies on certain issues discussed herein such as authorization for the use and disclosure of PHI, notice of DPH privacy practices, and patient rights. There is also a separate policy addressing the requirements the Privacy Rule places on research.

Another section of HIPAA contains a proposed "Security Rule." This proposed Security Rule focuses on ensuring that electronic health information that pertains to an individual remains secure. DPH has developed and updated other policies to address security issues. These policies address, among other issues, the maintenance and/or exchange of medical information via e-mail, fax, hand-held devices, and non-DPH personal computers and networks.

COMPARISON WITH EXISTING STATE LAWS

California also has a privacy statute known as the *California Confidentiality of Medical Information Act*. Further, other federal and state statutes provide additional protection for certain medical, mental health, and substance abuse information. DPH must comply with both the federal Privacy Rule and existing state laws. In situations where laws conflict or overlap, DPH must comply with the law that provides the patient with the greater protection or that restricts DPH procedures more. Determining which law applies can be complex; any questions should be referred to the DPH Privacy Officer.

4. Procedures

I. Use and Disclosure of PHI for Treatment, Payment, and Health Care Operations

- A. DPH providers, DPH staff, and DPH contract providers may use PHI for treatment, payment and health care operations. Use of information applies to internal sharing or utilization of PHI. Disclosure applies to the release of PHI to non-DPH providers or entities and is restricted as discussed in this policy.
- B. Treatment, payment and health care operations are defined as follows:
 - 1. **Treatment** means providing, coordinating, or managing a patient's care, including patient education and training, consultations between providers and referrals.
 - 2. **Payment** means activities related to being paid for services rendered. These activities include eligibility determinations, billing, claims management, utilization review, and debt collection.
 - 3. **Health care operations** means a broad range of activities such as quality assessment, student training, contracting for health care services, medical review, legal services, auditing functions, business planning and development, licensing and accreditation, business management, and general administrative activities.
- C. Divisions and units within DPH may identify higher standards regarding when an individual's signed release or other safeguards for the disclosure of PHI are required. Proposed higher standards must be reviewed and approved by the DPH Compliance Office.

II. Minimum Necessary Uses and Disclosures

- A. When using or disclosing PHI, or when requesting PHI from a non-DPH provider or entity, DPH providers and staff shall make reasonable efforts to limit the PHI requested, used, or disclosed to the minimum necessary to accomplish the patient's care.
- B. DPH shall identify those in its workforce who need access to PHI and limit access based on job scope and the need for the information.
- C. The *minimum necessary* requirement does not apply to the following:
 - 1. Disclosures to, or requests by, a DPH health care provider for treatment purposes;
 - 2. Uses or disclosures made to the individual treated, as permitted or required by law;
 - 3. Uses or disclosures made pursuant to the individual's authorization;
 - 4. Disclosures made to the Secretary of DHHS pursuant to an investigation or compliance review; and

5. Other uses or disclosures that are required by law, made pursuant to a subpoena or court order, or for workers' compensation purposes.

III. Special Requirements for Mental Health and Developmental Disability Information, Substance Abuse Information, Sexually Transmitted Disease Information, and Health Information of Minors

A. Mental Health Information

1. Although the federal privacy rule largely does not make a distinction between medical and mental health information, California state law does provide special protections for mental health information. Mental health information may be shared among DPH providers and contractors for the purposes of treatment. All other uses and disclosures require the specific authorization of the patient to disclose mental health information.
2. Mental health information includes process notes¹, medication prescription and monitoring, counseling session start and stop times, modalities/frequencies of treatment, results of clinical tests, or summaries of diagnosis, functional status, treatment plans, symptoms, prognosis, or progress recorded by mental health professionals.
3. Generally, disclosures of mental health information require the specific authorization from the patient for release. The state law that addresses the confidentiality of mental health information is the California Welfare and Institutions Code Section 5328 et seq., known as the Lanterman-Petris-Short Act ("LPS Act"). Questions regarding the use or disclosure of mental health information should be referred to the DPH Privacy Officer.

B. Substance Abuse Information

1. Although the federal Privacy Rule does not make a distinction between medical and substance abuse information, other federal statutes and California state laws do provide statutory restrictions for the release of information developed or obtained in the course of providing substance abuse treatment in federally funded substance abuse programs. Substance abuse information obtained in the course of general medical treatment is not subject to these provisions. Therefore, substance abuse information may be shared among DPH providers and to its contracted providers without authorization of the patient for patient care purposes. For example, substance abuse information may be shared from the General Medical Clinic to Castro-Mission Health Center or to a substance abuse program. However, the contracted substance abuse treatment program must obtain the patient's authorization to share information back to the General Medical Clinic or Castro-Mission Health Center. All other uses and disclosures require specific substance abuse authorization from the patient.
2. Information pertaining to substance abuse patients is subject to special protection under federal statute 42 U.S.C. Section 290dd-2 and under federal regulations found in the "Confidentiality of Alcohol and Drug Abuse Patient Records," 42 C.F.R. part 2. Additionally, California Health and Safety Code Section 11977 provides special protections to information of certain drug abuse programs. The LPS Act may also apply if the patient receives services such as involuntary evaluation and treatment because the patient is gravely disabled or dangerous to self or others as a result of abuse of alcohol, narcotics, or other dangerous drugs.

¹ DPH policy prohibits the use of psychotherapy notes.

3. These federal and state statutes require written authorization for disclosure of substance abuse information in certain circumstances and other special protections for substance abuse information. In these situations, the state law must be followed. Questions regarding the use or disclosure of substance abuse information should be referred to the DPH Privacy Officer.

C. HIV Test Results

Per state law HIV test results can not be disclosed without specific, written authorization from the patient except for purposes of diagnosis, care, or treatment of the patient by DPH providers.

D. Minors

Use and disclosure of protected health information associated with the care of minors should be administered using the same principles as consent for treatment. If the minor can consent for services per federal or state statute or DPH policy, then the minor controls his or her privacy rights.

Generally, a parent or assigned guardian controls a minor's privacy rights. However, there are a number of exceptions that apply in which a minor holds the right to consent and therefore controls all consequent privacy rights. These exceptions include the following:

1. Emancipated minors are those 14 years of age and older who have been emancipated by court order, are serving in the active U.S. military, or are married or have been married.
2. Self-sufficient minors are those youth 15 years of age or older living on their own, and managing their own financial affairs.
3. Minors 12 years of age or older receiving certain "sensitive services" regarding reproductive health, mental health, substance abuse, pregnancy, reportable diseases, rape, or sexual assault.
4. Minors 12 years of age or older who per DPH minor consent policy request and consent to a medical or behavioral health assessment without parental consent (see DPH policy and procedure "Consent for Dependent Minors"
<http://www.sfdph.org/dph/files/HIPAAdocs/PrivacyPolicies/MinorsConsentPol120622005.pdf>).

Please note that the attending professional should clearly document that the above criteria have been met if services are provided pursuant to these provisions of the law or DPH policy. See Community Behavioral Health Services policy and procedure "Consent for Voluntary Health Services: Minors" and DPH policy and procedure "Consent for Dependent Minors, Ages 12-17: Urgent, Primary Care and Behavioral Health Services."

IV. Disclosures to Family, Other Relatives, Close Personal Friends, and Personal Representatives

- A. DPH providers may disclose PHI to an individual's family members or other relatives, close personal friends, or any other person identified by the individual:
 1. upon the individual's oral agreement;
 2. if there is no objection when the individual is provided with an opportunity to object.

Note that minor consent rules apply if treatment is provided as described in section III D above. If oral agreement is obtained or no objection is raised, this must be recorded in the patient's medical record.

- B. Such disclosures shall be limited to information directly relevant to that person's involvement with the individual's care or payment for that care.
- C. If the individual is not present (e.g., the provider is in an outpatient setting) or is incapacitated, the provider may disclose information to family members, relatives, or close personal friends if the provider believes and can substantiate disclosure is in the best interest of the individual
- D. Generally, no information may be disclosed to a family member, relative, or close personal friend regarding mental health, substance abuse, or sexually transmitted disease, or HIV/AIDS services, or a developmental disability without the individual's specific authorization. This applies also to minors consenting to treatment under minor consent rules discussed in section III D above.
- E. DPH providers shall disclose information to an individual's personal representative (i.e. those granted legal authority to make health care decisions on behalf of another) in the same manner as they would for the individual.

V. Permitted Disclosures for Public Interest Related Purposes (See separate DPH Policy "HIPAA Compliance: Authorization for Use and Disclosure of Protected Health Information".)

- A. DPH providers and staff may disclose PHI without authorization for a variety of public interest-related purposes, including the following public health activities that involve safety or communicable disease:
 - 1. Reporting disease, injury, and vital events (e.g., birth or death);
 - 2. Conducting public health surveillance, investigations, and interventions;
 - 3. To report victims of abuse, neglect, or domestic violence to a public health or other government authority legally authorized to receive such reports;
 - 4. Judicial and administrative proceedings;
 - 5. Law enforcement purposes;
 - 6. Organ and tissue donations;
 - 7. National security and intelligence activities;
 - 8. Workers' compensation; and
 - 9. Requests related to decedents.
- B. Limitations regarding minimum necessary use, mental health and substance abuse information may apply to these public-interest related disclosures.

VI. De-Identified Information (See separate DPH policy "HIPAA Compliance: Privacy and the Conduct of Research")

- A. De-identified information may be used or disclosed as long as no means of re-identification is disclosed.
- B. In order to meet the definition of "de-identified" under the federal HIPAA Privacy Rule, all of the following specified identifiers must be removed: names, geographic designations smaller than a state (except for the initial three digits of zip codes if the first three digits cover an area having more than 20,000 people), dates (other than years), ages over 89 (although all persons over 89 may be aggregated into a single category), telephone and fax numbers, e-mail addresses, social security numbers, medical record numbers, health plan beneficiary

numbers, account numbers, certificate and license numbers, vehicle identification numbers, device identifiers and serial numbers, URLs and IP addresses, biometric identifiers, identifiable photographs, and any other unique identifiers.

- C. DPH providers and staff may disclose PHI to a business associate for the purpose of de-identifying such information. Business associate relationship exists when an individual or non-DPH entity, acting on behalf of the DPH, assists in the performance of a function or activity involving the use or disclosure of PHI. In order to have access to PHI, however, the business associate must have been formally recognized by DPH administration as such.
- D. If all of the required identifiers are not removed, information can still be treated as de-identified if a qualified statistician determines that the risk of re-identification is very small. This analysis must be documented.

VII. Authorization for Use and Disclosure (See separate DPH Policy "HIPAA Compliance: Authorization for Use and Disclosure of Protected Health Information.")

- A. DPH shall obtain an individual's authorization prior to the use or disclosure of PHI for reasons other than DPH treatment, payment or health care operations, or for purposes required by law.
- B. Common situations in which an individual's written authorization is required include disclosures to a life insurance company or an employer.
- C. Because it is focused on a particular use or disclosure, an authorization must be specific with regard to the information to be disclosed, who may disclose it, and who may receive it. It must also be time limited.
- D. Individuals may revoke their authorizations at any time if they do so in writing.
- E. DPH shall document and retain all authorizations for a minimum of seven years.
- F. Individuals have a right to a copy of authorizations signed at the request of DPH or one of its providers.
- G. DPH shall not deny treatment based on the refusal of an individual to authorize the use or disclosure of his/her PHI.
- H. Oral authorizations are permissible in the following circumstances:
 - 1. For an inpatient facility directory;
 - 2. For disclosure of information to family members, relatives, and close personal friends;
 - 3. To notify a family member, personal representative, or other person responsible for the care of an individual about the individual's location, general condition or death (if the patient has the capacity to make decisions, DPH shall obtain the individual's authorization or provide the individual with an opportunity to object); and
 - 4. To assist in disaster relief efforts.
- I. Clients may participate in program testimonials and promotions. The primary clinician (i.e. physician, nurse, therapist or counselor) should be contacted and give their approval prior to approaching a client to seek the client's participation. A client agreeing to give a program testimonial or become involved in a promotion must sign an *Authorization for Use and Disclosure of PHI* form prior to their participation in this activity.

VIII. Notice of Privacy Practices (See separate DPH policy " DPH Notice of HIPAA Privacy Practices")

- A. DPH shall describe, in plain language and in translation as required by the threshold languages list of the state of California, its privacy practices, including an individual's rights related to his or her PHI.
- B. This "Notice of Privacy Practices" shall be posted in prominent places in DPH care facilities and on the DPH web site.
- C. DPH will provide the notice to each of its patients (or their agents) upon their first encounter for health care services.
- D. DPH shall make a good faith effort to obtain a written acknowledgement from each individual who receives health care services that he/she received a copy of the Notice of Privacy Practices.
- E. Jail Health Services is exempted by the Privacy Rule from requirements to provide the "Notice of Privacy Practices."

IX. Patient Rights Regarding PHI (See DPH policy "HIPAA Compliance: Patient/Client/Resident Rights Regarding Protected Health Information.")

- A. DPH shall provide patients with certain rights pertaining to their PHI. These rights are as follows:
 - 1. The right to obtain a written notice explaining how DPH will use and disclose their information;
 - 2. The right to access their medical information (this includes seeing their records, requesting copies [paper, or , if available, electronic], requesting amendments to their records, authorizing sharing of health information, and getting an accounting of specified disclosures);
 - 3. The right to request that certain information be restricted from use or disclosure for purposes of treatment, payment, and health care operations (DPH may not grant this request if it is deemed unreasonable or overly burdensome);
 - 4. The right to request that information be communicated in particular ways to ensure confidentiality; and
 - 5. The right to refuse to authorize the release of PHI for purposes not related to treatment, payment, or health care operations or those required by law.
 - 6. The right to be notified of a breach.

X. Administrative and Operational Measures (See DPH policy "HIPAA Compliance: Administrative Requirements.")

- A. DPH shall implement administrative and operational measures to ensure compliance with the Privacy Rule as follows:
 - 1. Develop policies, procedures and systems to protect patient privacy;
 - 2. Train staff on these procedures;
 - 3. Appoint a Privacy Officer to make sure privacy procedures are developed, adopted, and followed;

4. Secure records that contain PHI and implement reasonable safeguards to limit access to PHI to those DPH employees whose jobs require such access.
5. Account for specified disclosures of PHI;
6. Establish a complaint mechanism for privacy concerns; and
7. Establish and enforce a system of sanctions for employees who violate privacy policies and procedures.

XI. Enforcement (See DPH policy "HIPAA Compliance: Administrative Requirements.")

- A. Each DPH employee is responsible for understanding and complying with this policy and the Privacy Rule. It is the responsibility of DPH managers and supervisors that appropriate privacy training is provided to all employees on an ongoing basis and that employees reporting to them are complying with DPH privacy policies.
- B. Any DPH employee who knows of, suspects, or has a question regarding a possible violation of the Privacy Rule may contact the DPH Privacy Officer. No employee shall be retaliated against for reporting a possible violation. If the employee wishes to remain anonymous, that employee may call the DPH Compliance Hotline at 415-642-5790 (CHN) or 415-252-3078 (PHP and Central Admin).
- C. DPH employees who violate the Privacy Rule shall be disciplined through the civil service process and in accordance with the applicable Memorandum of Understanding. Discipline may involve actions up to and including termination of employment.
- D. The federal Office for Civil Rights ("OCR") of the Department of Health and Human Services will enforce the Privacy Rule on behalf of the federal government. DPH employees, patients, and clients may file a complaint with the OCR and are not required to use the DPH complaint process.
- E. There are both civil monetary penalties and criminal sanctions for violations of the Privacy Rule.
- F. If a DPH provider or other employee is found to have violated any of the privacy standards, he/she may be penalized up to \$100 for each violation. If a DPH provider or other employee is found to have repeatedly violated the exact same requirement or prohibition, the government cannot impose a fine of more than \$25,000 in a single year. Additional fines may be imposed pursuant to state law.
- G. Criminal sanctions, including larger fines and imprisonment, may be imposed for knowingly disclosing or obtaining PHI in violation of the Privacy Rule.

5. References/Attachments

1. DPH Policy "HIPAA Compliance: Authorization for Use and Disclosure of Protected Health Information" – *see attached*.
2. DPH policy "[HIPAA Compliance: Privacy and the Conduct of Research](#)"
3. DPH policy "[DPH Notice of HIPAA Privacy Practices](#)"
4. DPH policy "[HIPAA Compliance: Patient/Client/Resident Rights Regarding Protected Health Information](#)"
5. DPH policy "HIPAA Compliance: Administrative Requirements" – *see attached*.



City and County of San Francisco

Edwin M. Lee, Mayor

San Francisco Department of Public Health

Barbara A. Garcia, MPA
Director of Health

DPH PRIVACY POLICY: ATTACHMENT 1

San Francisco Department of Public Health

*Policy & Procedure Detail**

Policy & Procedure Title: Authorization for Use and Disclosure of Protected Health Information	
Category: Privacy	
Effective Date: 4/2003, Revised 2/24/2010	Last Reissue/Revision Date: 9/23/2013
DPH Unit of Origin: SFDPH Privacy Office	
Policy Contact - Employee Name and Title; and/or DPH Division: Alice Gleghorn, Ph.D., SFDPH Privacy Officer	
Contact Phone Number(s): 415-255-3722	
Distribution: DPH-wide X	If not DPH-wide, other distribution:

**All sections in table required.*

1. Purpose of Policy

To comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule, as well as relevant state and federal laws controlling the release of PHI, by establishing a process to obtain proper authorization for the use or disclosure of protected health information (PHI) when necessary and appropriate.

2. Policy

It is the policy of the San Francisco Department of Public Health (DPH) to comply with the HIPAA and all other applicable state and federal confidentiality laws by obtaining authorization before using or disclosing PHI, unless the use or disclosure is specifically permitted or required by law.

SCOPE

This policy pertains to all individuals who may access, use, or disclose DPH PHI. DPH divisions or units may enforce stricter authorization requirements for the use or disclosure of PHI than those set forth in this policy.

3. Definitions

- A. **Protected Health Information (PHI):** Individually identifiable health information maintained or transmitted in any medium.

The mission of the San Francisco Department of Public Health is to protect and promote the health of all San Franciscans.

We shall ~ Assess and research the health of the community ~ Develop and enforce health policy ~ Prevent disease and injury ~
~ Educate the public and train health care providers ~ Provide quality, comprehensive, culturally-proficient health services ~ Ensure equal access to all ~

- B. **Use:** The sharing, employment, application, utilization, examination, or analysis of protected health information within DPH, its affiliates, or its contract providers.
- C. **Disclosure:** To release, transfer, provide access to, or divulge in any other manner protected health information.
- D. **Authorization:** The formal consent document releasing PHI from the records of an entity covered by the privacy provisions of HIPAA.

4. Procedures

I. MINIMUM NECESSARY RULE

- A. General Rule: When disclosing PHI, or when requesting PHI from another covered entity, providers must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.
- B. Exceptions
 1. Disclosures for, or uses related to, treatment (see Attachment A – DPH Privacy Policy Matrix – Sharing Protected Health Information for Treatment Purposes);
 2. Disclosures to the patient or patient representative pursuant to patient access rights;
 3. Uses or disclosures made pursuant to a valid HIPAA authorization which describes the PHI to be disclosed;
 4. Disclosures made to the Secretary of the United States Department of Health and Human Services pursuant to an investigation or compliance review; and
 5. 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).

II. ADMINISTRATION OF AUTHORIZATIONS

- A. **An authorization is required in the following situations** (see Attachment A – DPH Privacy Policy Matrix – Sharing Protected Health Information for Treatment Purposes):
 1. Per the HIPAA Privacy Rule for use of PHI by DPH, its providers, its affiliates and its contract providers for purposes not related to treatment, payment, or health care operations.
 2. Per 42 CFR Part 2, for the disclosure of information pertaining to an individual's treatment in a substance abuse program, except in a medical emergency.
 3. Per CCSF Local Share Mandate established with the California Office of AIDS, for the disclosure of information pertaining to an individual's treatment in a CCSF HIV Health Service program outside that network of providers.

B. Valid Authorization Forms

1. When authorization is required, all DPH divisions/units and providers shall obtain patient/client/resident authorization using the standard DPH Authorization to Release Protected Health Information form.
2. Due to strict HIPAA requirements for an authorization form to be valid (see [Attachment B](#)); any DPH provider that plans to develop a different authorization form must have that form approved by a DPH Privacy Officer.
3. Authorizations for use or disclosure of PHI received from other persons, providers, or agencies requesting information from DPH must contain all of the HIPAA-required elements. Inadequate authorizations should be returned to the sender.
4. All researchers who request permission to conduct a study with human subjects in the DPH must include with the request a DPH standard authorization for the use of the PHI generated from the study. This standard authorization must contain all elements required by HIPAA. Refer to DPH Privacy Policy "Conduct of Research" for more information.

C. Invalid Authorizations

An authorization is not valid if:

1. The expiration date has passed or the expiration event is known by DPH to have occurred;
2. The authorization has not been filled out completely;
3. The authorization is known by DPH to have been revoked;
4. Material information in the authorization is known by the DPH to be false;
5. The authorization was improperly combined with another document; or
6. The authorization is not in 14-point font type.

D. Documenting Authorizations

1. All authorizations for use and disclosure of DPH PHI should be filed in the correspondence section of the medical record of the individual concerned.
2. A copy of the completed authorization form should be offered to the patient/resident/client.

E. Compound Authorizations

1. General Rule: DPH authorizations may not be combined with any other document to create a "compound authorization."
2. **Exception: An authorization for the disclosure of DPH PHI generated by research may be combined with the required informed consent for participation in the research.**

F. Making Treatment, Payment, Enrollment, or Eligibility Conditional Upon an Authorization

1. General Rule

- a. DPH shall not make treatment, payment, enrollment in a health plan or eligibility for benefits conditional upon the patient, resident or client's execution of an authorization.
2. Exceptions
 - a. For treatment as part of research in which the individual will participate as a human subject.
 - b. When the purpose is to create DPH PHI to disclose to a third party (e.g., pre-enrollment physicals).
 - c. When the program is designed for a specific population whose participation is conditional upon authorization (e.g., Behavioral Health Court).
 - d. A DPH-sponsored or DPH-affiliated health plan may make enrollment or eligibility for benefits conditional upon authorization, provided that the authorization (i) is obtained prior to enrollment and (ii) relates specifically to the individual or to underwriting or risk-rating determinations.

III. ORAL AGREEMENTS

DPH may rely upon an individual's oral approval to disclose, restrict or prohibit the use of PHI under the following circumstances:

- A. For an inpatient or resident facility directory;
- B. For involvement in the individual's care by next-of-kin, family members, domestic partners, and/or close personal friends; and
- C. To notify a family member, personal representative or other person responsible for the care of the individual about the individual's location, general condition, or death.

V. MINORS

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

- A. Emancipated (Married, Active Military Service, By Court Order); or
- B. Self-Sufficient (age 15 or older, living separate and apart from parents, managing own finances) if relative to General Medical and Dental Care; or
- C. By law, is allowed to give own consent to "Sensitive Services." Criteria for that includes:
 1. Any-Age Minor: Care related to the prevention or treatment of pregnancy, sexual assault or rape,
 2. Minor age 12 and older: Outpatient mental health (if "at risk" criteria are met), outpatient drug and alcohol, treatment of infectious, contagious or communicable reportable disease or sexually transmitted disease, HIV testing and treatment.

VI. DECEASED CLIENTS/PATIENT

For deceased clients/patients, the patient representative (next of kin or executor of estate) has the rights that the patient would have had relative to access and release of the record.

VI. EMPLOYMENT DETERMINATIONS

Authorization is required for DPH to use or disclose an individual's PHI for employment determinations. For example, DPH must have the individual's authorization to disclose the results of a pre-employment physical to an individual's employer.

VII. VERIFICATION PROCEDURES

Prior to making any disclosures permitted by HIPAA, staff shall verify the identity of the person requesting DPH PHI and the authority of any such person to have access to DPH PHI.

VIII. MEDIA AND OTHER INQUIRIES

- A. All media inquiries should be referred immediately to a DPH Privacy Officer and/or the DPH Public Information Officer prior to release of information.
- B. No information may be disclosed if the patient has requested that information be withheld. Otherwise, the condition of an inpatient, outpatient, or emergency patient to the media may be disclosed **only if** the inquiry specifically contains the patient's name. (See exclusion in F and G below.)
- C. A DPH patient's condition may be described only in general terms that do not communicate specific medical information about the individual (e.g., undetermined, good, fair, serious, critical, or deceased).
- D. Care should be taken to first notify the DPH patient's next of kin before the fact of death is made public. No additional information about a patient's death, including the cause, date, or time of death, may be made without written authorization from a legal representative of the deceased patient, even if this information has been disclosed to the Medical Examiner or the Death Registrar.
- E. Information concerning a DPH patient's location in the hospital may be made to facilitate visits by family or friends or for delivery of gifts or flowers if the inquiry includes the patient's name and there is no instruction from the patient to withhold such information. This information should not be routinely disclosed to the media.
- F. As standard practice, DPH does not release information to the media about identifiable DPH clients engaged in behavioral health services (including those served in outreach, mental health, substance abuse, HIV, or supportive housing programs). This policy applies to current, previous, and deceased clients.
- G. Per DPH policy, brochures, or publications developed by DPH-funded programs are not to include identifiable clients in photos or personal stories that disclose their current or past mental health issues or substance use, or engagement in behavioral health services unless the client has specifically requested to participate in testimonials, promotions, and other materials, and has signed an authorization allowing this use. Programs should consult with the primary clinician before approaching a client about potential participation in this type of activity. A client agreeing to give a program testimonial or become involved in a

promotion must sign an Authorization for Use and Disclosure of PHI form prior to their participation in this activity.

IX. PERMISSIBLE DISCLOSURES WITHOUT AUTHORIZATION FOR PUBLIC POLICY PURPOSES

An authorization is not required in the following situations:

- A. For disclosures required by state or federal law.
- B. For DPH public health activities specifically permitted or required by law, such as preventing and controlling disease, injury, or disability; providing information to the Food and Drug Administration regarding adverse drug events, tracking health-related products, enabling product recalls, or conducting post-marketing product surveillance.
- C. For a work-related injury or illness when the release is to the responsible employer (the individual must be informed of the disclosure); that is, the employer has sent the patient, is paying for the care under workers comp, etc.
- D. For reporting victims of abuse or neglect as specifically required under the law.
- E. For reporting to a health oversight agency regarding activities authorized by law, including civil, administrative or criminal investigations, proceedings, actions, or inspections, audits, licensure surveys or investigations, or disciplinary actions.
- F. For responding to an order of a court or administrative tribunal issuing a subpoena, discovery request, or other lawful process.
- G. For providing the San Francisco Medical Examiner or a funeral director with information needed to carry out his or her duties as authorized by law.
- H. For facilitating organ, eye, or tissue donation, and transplantation.
- I. For preventing or lessening a serious and imminent threat to the health or safety of a person or the public when the individual to whom the disclosure is made is capable of preventing or lessening the threat.
- J. To warn reasonably identifiable victim(s) and notify law enforcement when a client communicates a serious threat of violence against a reasonably identifiable victim or victims (Tarasoff Duty to Warn).
- K. For informing the Department of Veterans Affairs as authorized by law of information needed for determination of eligibility or entitlement to benefits for an individual following discharge from military service.
- L. For disclosing information as authorized by law to provide benefits for work-related injuries and illnesses.

X. PERMISSIBLE DISCLOSURES WITHOUT AUTHORIZATION FOR CARE COORDINATION PURPOSES NOT OTHERWISE COVERED.

- A. As of January 1, 2009, 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 protected health information 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.).

XI. PERMISSIBLE DISCLOSURES OF GENERAL HEALTH INFORMATION WITHOUT AUTHORIZATION FOR LAW ENFORCEMENT PURPOSES

An authorization is not required in the following situations:

- A. When the disclosure of PHI is made in response to a law enforcement official's request for such information for the purpose of IDENTIFYING or LOCATING a suspect, fugitive, material witness, or missing person and the PHI is limited to:
- (a) Name and address
 - (b) Date and place of birth
 - (c) Social Security number
 - (d) ABO blood type and Rh factor
 - (e) Type of injury
 - (f) Date and time of treatment
 - (g) Date and time of death, if applicable
 - (h) Description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars, and tattoos
- B. PHI related to an individual's DNA, DNA analysis, dental records, or typing, sampling, or analysis of body fluids or tissues MAY NOT be disclosed, excluding ABO blood type and Rh factor.
- C. When the disclosure of PHI is made in response to a law enforcement official's request for such information about an individual who is or is suspected to be a victim of a crime, provided that:
1. The law enforcement official represents that immediate law enforcement activity that depends on the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure, and
 2. The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred and such information is not intended to be used against the victim.
- D. When the disclosure is made to a law enforcement official about a decedent suspected to have died as the result of criminal conduct, excluding Mental Health clients (unless in a state hospital).

- E. When the disclosure is made to a law enforcement official about an individual, the PHI of whom constitutes evidence of criminal conduct that occurred on the premises of DPH.
- F. When the disclosure is made to a law enforcement authority to identify or apprehend an individual because of a statement made by the individual admitting participation in a violent crime that caused serious harm to a victim, excluding mental health information.
- G. When the disclosure is made to a law enforcement authority where it appears from all circumstances that the individual has escaped from a correctional institution or from lawful custody.
- H. When the disclosure is made to a correctional institution or law enforcement official having lawful custody of an inmate or other individual for:
 - (a) The provision of healthcare to such individual (disclosures may include mental health or HIV information as well);
 - (b) The health and safety of such individual or other inmates;
 - (c) The health and safety of the officers or employees or of others at the correctional institution;
 - (d) The health and safety of individuals and officers responsible for the transport or transfer of inmates from one correctional or health care setting to another;
 - (e) Law enforcement on the premises of the correctional institution; or
 - (f) The administration and maintenance of the safety, security, and good order of the correctional institution.

5. References/Attachments

1. **Attachment A:** City and County of San Francisco Department of Public Health DPH Privacy Policy Matrix – Sharing Protected Health Information for: Treatment Purposes
2. **Attachment B:** Required Elements of an Authorization to Release Protected Health Information Form

Attachment A

City and County of San Francisco Department of Public Health
DPH Privacy Policy Matrix – Sharing Protected Health Information for:

TREATMENT PURPOSES

When allowed by law (see below), Protected Health Information (PHI) may be shared for treatment purposes across disciplines and programs on a “need-to-know” basis and for the purposes of improving health outcomes. PHI includes case management/coordination communication, medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment, results of clinical tests, and any summary of the following items: diagnosis, functional status, treatment plan, symptoms, prognosis, and progress to date.

Description of PHI	Who may disclose it?	Who may receive it?
General Health (includes knowledge of Mental Health, Substance Use/Abuse, HIV/AIDS, STD conditions)	General Health Provider	Patient's providers and providers' staff for the purpose of treatment, diagnosis, or referral <i>[Reference: Civil Code 56.10(a); HIPAA Treatment Exception]</i>
Mental Health (includes knowledge of General Health, Substance Use/Abuse, HIV/AIDS, STD conditions)	Mental Health Provider	Any healthcare provider (any discipline) "who has medical or psychological responsibility for the patient" <i>[Reference: W&I Code 5328(a); HIPAA Treatment Exception]</i>
Drug/Alcohol Treatment Program (includes knowledge of General Health, Mental Health, HIV/AIDS, STD Conditions)	Drug/Alcohol Treatment Program Provider	<u>Only</u> another member of the client's treatment team <u>WITHIN</u> the specific drug/alcohol treatment program Exception: a medical emergency <i>[Reference: 42 CFR Part 2, section 2.12 (c)(3)]</i>
HIV/AIDS CCSF Health Service Provider Network (includes knowledge of General Health, Mental Health, Substance Use/Abuse, STD conditions)	HIV/AIDS CCSF Health Service Provider	<u>Only</u> another HIV Health Service provider who registers client in ARIES database. <i>[Reference: CCSF Local Share Mandate established with the California Office of AIDS]</i>

Revised 01-05-10 and 12-19-13

Treatment Providers

Individual practitioners and program staff in agencies that furnish health services in the normal course of their business are considered treatment or healthcare providers.

HIPAA defines treatment as "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." References: Civil Code 56.10(c)(1), H&S Code 123010, and HIPAA (45 CFR sec.164.506, 45 CFR 164.501 45, CFR 164.506).

For purposes of care coordination and treatment, healthcare providers may be inside or outside the DPH Safety Net, but they and/or their agencies must be bound by state and federal confidentiality laws and/or DPH MOUs to be considered a "treatment provider" as noted in the above matrix.

The DPH Safety Net includes civil service, contract, and affiliate programs (such as those of UCSF and the SF Community Clinic Consortium).

The following are some examples of other treatment providers whose clients' PHI may be shared for treatment and coordination purposes without an authorization:

1. Individual practitioners and treatment providers of private sector hospitals and clinics who are bound by state and federal confidentiality laws.
2. Providers who sell or dispense drugs, devices, equipment, or other items in accordance with a prescription.
3. (via MOU) Paramedics of the San Francisco Fire Department EMS
4. (via MOU) Case managers in the Human Services Agency Homeless Programs:
 - a. HSA Behavioral Health Roving Team
 - b. Housing Access Team
5. (via MOU) Case managers in the Department of Aging and Adult Services Case Management Programs:
 - a. Bernal Heights Neighborhood Center's
 - b. Neighborhood Elders Support Team (NEST) Case Management Program
 - c. Active Senior Case Management Program
 - d. Episcopal Community Services' Canon Kip Senior Center Case Management Program
 - e. Curry Senior Center Case Management Program
 - f. DAAS Adult Protect Services (APS) Case Management Program
 - g. Family Service Agency Seniors Case Management Program
 - h. IHSS (In Home Supportive Services) Consortium Case Management Program
 - i. Institute on Aging
 - j. MSSP (Multipurpose Senior Services) Case Management Program
 - k. Linkages Case Management Program
 - l. District Wide Social Services/District 5 Case Management Programs serving Mission, Noe Valley, Bernal Heights, Buena Vista, and Eureka Valley
 - m. Neighborhood Resource Centers Case Management Programs serving Richmond District, Western Addition and the Mission
 - n. Meals on Wheels Case Management Program
 - o. San Francisco Senior Centers Case Management Programs
 - p. Self-Help for the Elderly Case Management Program
 - q. On Lok 30th Street Senior Services Case Management Program
6. (via MOU) Care Coordinators of the San Francisco Health Plan

Questions about who is and who is not a health service provider should be directed to your Privacy Officer.
[revised mxm 031313]

Attachment B:

REQUIRED ELEMENTS OF AN AUTHORIZATION TO RELEASE PROTECTED HEALTH INFORMATION FORM

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 on 8 ½ x 11-inch paper and the font size must be at least 14 points.

HIPAA, state law, and DPH policy require that each patient’s authorization include certain core elements as follows:

1. Patient/Client’s name and date of birth
 2. Name of the disclosing entity/facility
 3. Name and address of the facility/individual to receive the protected health information
 4. Description of the information to be disclosed
 5. Description of the purpose of the disclosure
 6. Expiration date or the condition upon which authorization is terminated
 7. The patient or client’s initials next to the types of PHI being released in a “protected classes” section for release of:
 - a. mental health information,
 - b. substance abuse information,
 - c. HIV/AIDS information,
 - d. developmental disabilities,
 - e. sexually transmitted disease information.
 8. Completed statements where client/patient acknowledges the following:
 - a. I understand that authorizing the disclosure of this health information is voluntary. I may refuse to sign this authorization.
 - b. I understand that I may not be denied treatment, payment, enrollment in a health plan or eligibility for benefits if I refuse to sign.
 - c. I understand that I have a right to receive a copy of this authorization.
 - d. I understand that my authorization to use or disclose protected health information expires on _____ or until _____ condition is met.
 - e. 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 forward, and not retroactively.
 - f. 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.
 9. Signatures and Dates
 - a. Patient/Client
 - b. Parent/Guardian/Conservator if patient/client is unable to sign
 - c. Witness, if patient/client is unable to sign
-
-



City and County of San Francisco

Edwin M. Lee, Mayor

San Francisco Department of Public Health

Barbara A. Garcia, MPA
Director of Health

DPH PRIVACY POLICY: ATTACHMENT 5

TITLE: DPH Policy HIPAA Compliance: Administrative Requirements

PURPOSE

It is the policy of the San Francisco Department of Public Health (DPH) to adopt administrative policies and implement procedures that fulfill the administrative requirements set forth in the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The purpose of this administrative policy is to provide DPH with general administrative policies and procedures that, in accordance with the HIPAA Privacy Rule, help secure the privacy of health information and protect the privacy rights of individuals who have entrusted their protected health information (PHI) to the DPH.

SCOPE

This policy covers all DPH divisions and units and applies to all personnel working at DPH Facilities.

BACKGROUND

HIPAA requires DPH to adopt and implement administrative policies and procedures designed to secure the privacy of health information and protect the privacy rights of individuals who have entrusted their PHI to DPH.

PROCEDURE

I. PERSONNEL ASSIGNMENTS

- A. DPH shall designate a Privacy Officer responsible for developing and implementing policies and procedures regarding HIPAA.
- B. DPH shall designate a Privacy Officer responsible for receiving complaints from individuals who believe that DPH has violated federal or state laws governing PHI.
- C. This administrative policy documents the DPH designated personnel.

II. TRAINING

- A. Responsibility
 1. Department of Public Health
 - a. It is the responsibility of the San Francisco Department of Public Health, through the Privacy Officer, to provide privacy training to all DPH personnel who produce, transcribe, store, transmit or otherwise have access to PHI.
The training shall consist of but not be limited to:
 - (a) basic health privacy awareness training at new workforce member orientation;
 - (b) on-line specialized health privacy training where accessible;
 - (c) in-service specialized health privacy training where on-line training is unavailable;

The mission of the San Francisco Department of Public Health is to protect and promote the health of all San Franciscans.

We shall ~ Assess and research the health of the community ~ Develop and enforce health policy ~ Prevent disease and injury ~
~ Educate the public and train health care providers ~ Provide quality, comprehensive, culturally-proficient health services ~ Ensure equal access to all ~

(d) printed, electronic and in service consulting resources made available through the Compliance Office of the DPH.

2. Department Managers and Supervisors

- a. Department managers and supervisors are responsible for verifying that personnel who report to them have obtained health information privacy training sufficient to perform their duties in compliance with state and federal health privacy regulations, DPH health information privacy policy and health information privacy procedures.
- b. Department managers and supervisors are responsible for providing and/or requesting specialized health information privacy training for personnel who report to them.
- c. Department managers and supervisors are responsible for identifying and notifying the DPH Privacy Officer of any unmet health information privacy requirements within their departments.

3. DPH personnel

- a. DPH personnel are responsible for obtaining basic health information privacy training at new workforce member orientation and any specialized health information privacy training brought to their attention by their managers or supervisors;
- b. DPH personnel are responsible for notifying their managers or supervisors of any unmet specialized health information privacy training needs that come to their attention.

B. Training Documentation

1. DPH is responsible for documenting that personnel have completed privacy training.

III. COMPLAINTS TO DPH

A. Policy

1. DPH shall establish and maintain a process for individuals to register complaints regarding its privacy policies and procedures and/or its compliance with those policies and procedures. Individuals may call the DPH Privacy Officer, write the DPH Privacy Officer, or anonymously leave a message on the DPH Compliance Hotline at 415-642-5790 (CHN) or 415-252-3078 (PHP).
2. DPH shall document all complaints received regarding management of PHI and document the disposition of those complaints. Documentation shall be retained by DPH as required by law.
3. DPH shall not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual who files a complaint with DPH or with the Department of Health and Human Services.

B. Complaint Process.

1. *Communicating Process to Individuals.* DPH's Notice of Privacy Practices shall direct individuals to submit a complaint regarding management of PHI to the DPH Privacy Officer. The Notice shall also indicate that a complaint can be made directly to the Secretary of Health and Human Services (HHS).
2. The DPH Privacy Officer shall receive and review all complaints to DPH regarding the management of an individual's protected health information. Within ten (10) working days, the Privacy Officer shall notify the individual in writing of the disposition of the complaint.
3. *Disposition of Complaint.*

- a. **No Action Taken.** If the review determines that the complaint is without merit, no action will be taken. This disposition shall be noted on the complaint form and the client so informed.
- b. **Further Investigation Required.** If the Privacy Officer determines that a breach of policy or procedure has occurred or that the complaint identifies a potential for process improvement, the individual shall be notified that further review of the complaint is required and a final disposition will be delivered at a later date. The Privacy Officer shall refer the complaint to the appropriate department for follow-up (e.g. human resources for investigation of the breach and possible sanctions; or quality improvement for review and possible modification to a process). When the investigation has been completed and the matter resolved, the Privacy Officer shall notify the individual. If a breach of policy or procedure has resulted in an unauthorized use or disclosure of PHI, the Privacy Officer shall immediately implement steps to mitigate any potential harm to the individual.

4. All complaints to DPH regarding DPH management of PHI and documentation of the disposition of those complaints shall be filed in the office of the DPH Privacy Officer in a manner conducive to retrieval for review and/or audit. The documentation shall be retained for a period of six years from the date of the complaint.

IV. POLICIES AND PROCEDURES

- A. DPH shall develop, implement and enforce policies and procedures consistent with the Health Insurance Portability and Accountability Act of 1996.
- B. When necessary, DPH will revise these policies and procedures and update its training program to reflect these revisions.
- C. DPH shall document all procedures consistent with state and federal requirements.

V. ADMINISTRATIVE SAFEGUARDS TO PROTECT PHI

- A. The DPH Privacy Officer shall work collaboratively with the Chair of the DPH Data Governance Committee to insure that proper safeguards are in place to insure the use, access and disclosure of PHI is consistent with HIPAA, Federal, State, and local regulations
- B. These safeguards shall include (but are not limited to) effective review and audit protocols to monitor individual, use, access and disclosure of PHI maintained in any form across DPH.
- C. The Privacy Officer shall be responsible for recommending statistically valid sampling techniques and procedures to the Data Governance Committee to routinely test for inappropriate use, access or disclosure of PHI.
- D. The DPH Privacy Officer shall report monthly to the Data Governance Committee on the results of the application of these sampling techniques and procedures.

Date Adopted: 04/2003