[GO TO END]
[TOP]

Policy Number: 8.5

TITLE: HIPAA COMPLIANCE: PRIVACY POLICY

PURPOSE

The purpose of this policy is to provide guidance to providers and other DPH employees by setting forth the basic requirements for protecting the confidentiality of medical information as required by the Privacy Rule.

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 have access to, 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.

BACKGROUND

The federal Health Insurance Portability and Accountability Act of 1996 established through its Administrative Simplification regulations to assure 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. 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 will develop and/or update other policies to address security issues. These policies will 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.

PROCEDURE

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 psychotherapy notes, 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.

Generally disclosures of mental health information requires 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 treatment provided 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 treatment information may be shared from the General Medical Clinic to Castro-Mission Health Center or to a substance abuse provider contracted by Community Programs. However, the contracted substance abuse provider 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.
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. Sexually Transmitted Diseases and HIV/AIDS Information

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.

Per DPH policy, PHI from City Clinic (Municipal STD Clinic) and Community Health Epidemiology unit is only disclosed upon the specific authorization of the patient when not used for communicable disease monitoring and reporting purposes.

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').

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 "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:

1. Public health activities that involve safety or communicable disease;
2. To report victims of abuse, neglect, or domestic violence;
3. Judicial and administrative proceedings;
4. Law enforcement purposes;
5. Organ and tissue donations;
6. National security and intelligence activities;
7. Workers' compensation; and
8. 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 'Research and Use of PHI')

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 "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.

VIII. Notice of Privacy Practices (See Appendix A-1 "Summary DPH Notice of HIPAA Privacy Practices" and Appendix A-2 "Notice of Privacy Practices." and Summary)

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 "Patient 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, requesting amendments to their records, 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.

X. **Administrative and Operational Measures (See DPH policy "HIPAA 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 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.

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.

APPENDICES

Appendix A-1 "Summary DPH Notice of HIPAA Privacy Practices"
Appendix A-2 " DPH Notice of HIPAA Privacy Practices"

CROSS REFERENCE

SFGHMC Administrative P&Ps:
16.4 Patient Rights and Responsibilities

APPROVAL:

NEC:	5/05/09
MEC:	5/07/09
Quality Council	5/19/09

Date Adopted: 03/2003
Date Reviewed: 04/06, 5/09
Date Revised:

[GO TO TOP]

[END]