

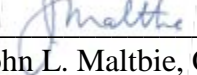


ADMINISTRATIVE MEMORANDUM COUNTY OF SAN MATEO

NUMBER: B-25

SUBJECT: Privacy Policy pursuant to the Health Insurance Portability and Accountability Act (HIPAA) of 1996, 45 C.F.R. §164.105(c)), as amended and supplemented by Subtitle D of the Health Information Technology for Economic and Clinical Health Act (HITECH Act) of the American Recovery and Reinvestment Act of 2009 and the HIPAA Omnibus Rule, 78 Fed. Reg. 5565 (Jan. 25, 2013), amending C.F.R. Parts 160 and 164.

RESPONSIBLE DEPARTMENT: County Manager / Clerk of the Board

APPROVED: 
John L. Maltbie, County Manager

DATE: June 26, 2014

I. INTRODUCTION

The federal Health Insurance Portability and Accountability Act of 1996, HIPAA, was established, through its Administrative Simplification regulations, to assure privacy for individuals receiving health care services in the United States. The “Privacy Rule” established by HIPAA created a national standard for minimum levels of protection for medical information and expanded consumer control over medical information.

The County of San Mateo (the “County”) collects and maintains protected health information (PHI) about its patients and health plan members (“Members”). These functions define the County as a covered entity that is subject to federal HIPAA laws and regulations. HIPAA regulations on privacy and confidentiality (45 CFR 160 et seq.) (“HIPAA regulations”) require that the County maintain the privacy of its patients’ and members’ PHI and limit how the County uses and discloses this information. Further, the Health Information Technology for Economic and Clinical Health (HITECH) Act is implemented through the revised HIPAA Omnibus Rule. *See* 45 C.F.R. Parts 160 and 164. This memorandum supersedes and replaces Administrative Memorandum B-25 dated April 14, 2003.

HIPAA regulations also provide patients and members with certain rights with respect to their PHI. In order to protect the privacy and confidentiality of the County’s patients’ and members’ PHI and to comply with federal law, all County workforce members who have access to, use, or disclose protected health information are required to comply with the provisions of this policy.

This policy is administered by the County's Privacy Officer in collaboration with the County Manager's Office and County Counsel.

This Privacy Policy applies to all County healthcare components, as designated by Administrative Memorandum B-26. In some cases, individual County health care components may wish to develop internal policies and procedures in compliance with HIPAA regulations and this policy. It is the responsibility of each County healthcare component to determine whether or not it is appropriate to develop such individualized internal policies and procedures in addition to this Policy.

The County understands that HIPAA privacy regulations set forth a minimum federal standard. California also has a privacy statute, the California Confidentiality of Medical Information Act ("CMIA"). In situations where state and federal law overlap, the County must comply with the law that provides patients with the higher degree of privacy protection. Determination of which law applies is complex and questions regarding application should be directed to the County's Privacy Officer.

I. DEFINITIONS

A. Business Associate means a person or entity other than a County employee that, on behalf of the County, acts in a capacity to assist the County in carrying out covered functions including but not limited to: claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and re-pricing. A Business Associate may create, receive, maintain or transmit PHI.

B. County of San Mateo (County), for the purposes of this Administrative Memo, includes, but is not limited to healthcare providers, including doctors, nurses, physician assistants, and nurse practitioners, as well as all other relevant personnel and contractors who come into contact with Protected Health Information (PHI).

C. Covered Function applies to functions which include, but are not limited to, healthcare services, health plan services and their respective support services such as collecting overdue debts, handling delinquent accounts, performing internal audit functions, maintaining databases, systems and infrastructure management with the potential for access to PHI, performing risk management functions, and legal services.

D. Disclosure means 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.

E. Protected Health Information (PHI) means information that (1) is created or received by the County; (2) relates to the past, present, or future physical or mental health or condition of a patient or member; the provision of healthcare to a patient or member; or the past, present, or future payment for the provision of healthcare to a patient or member; and (3) identifies the patient or member, or there is a reasonable basis to believe the information can be used to identify the patient or member. PHI includes information of persons both living and deceased.

The following identifiers of a patient's or member's information also are considered PHI and therefore must be treated like any other PHI:

- i. Names;
- ii. Street address, city, county, precinct, zip code;
- iii. Dates directly related to a patient or member, including birth date, admission date, discharge date, and date of death;
- iv. Telephone numbers, fax numbers, and electronic mail addresses;
- v. Social Security numbers;
- vi. Medical record numbers;
- vii. Health plan beneficiary numbers;
- viii. Account numbers;
- ix. Certificate/license numbers;
- x. Vehicle identifiers and serial numbers, including license plate numbers;
- xi. Device identifiers and serial numbers;
- xii. Web Universal Resource Locators (URLs) and Internet Protocol (IP) address numbers;
- xiii. Biometric identifiers, including finger and voice prints;
- xiv. Full face photographic images and any comparable images; and
- xv. Any other unique identifying number, characteristic, or code.

F. Treatment, Payment and Health Care Operations:

- i. **Treatment** means providing, coordinating or managing a patient's care, including patient education and training, as well as consultations between providers and the provision of referrals.

- ii. **Payment** means activities related to the County receiving payment for services rendered. Payment activities include, but are not limited to, eligibility determinations, billing, claims management, utilization review, and debt collection.
- iii. **Health Care Operations** are certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment. This definition includes a broad range of activities such as quality assessment, 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. *See* 45 CFR 164.501.

G. Workforce means employees, temporary employees, leased employees, volunteers, trainees, and other persons whose work performance is under the direct control of the County, whether or not they are paid by the County.

II. USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION (PHI)

County Providers and staff may use PHI for treatment, payment, and health care operations without patient authorization. Use of PHI applies to internal sharing or utilization of PHI. Disclosure applies to the release of PHI to non-County Providers or entities and is restricted as discussed in this policy.

A. Authorization. Except for situations outlined in this Privacy Policy, County providers will not use or disclose a patient's or member's PHI for any purpose without an authorization signed by the patient or member in accordance with 45 CFR 164.508(a)(1). A valid authorization must include the following elements:

- i. A description of the information to be used or disclosed;
- ii. The name or other specific identification of person or class of persons authorized to make the disclosure;
- iii. The name or other specific identification of person or class of persons to whom the disclosure may be made;
- iv. A description of each purpose of the requested disclosure;
- v. An expiration date; and
- vi. The signature of the patient or personal representative; if the authorization is signed by a personal representative of the patient, a description of the representative's authority to act for the individual must be produced.

The authorization must be in plain language and the person signing the authorization must be offered a copy of the signed authorization. The patient or member has the right to revoke an authorization in writing at any time, except to the extent that the County may have already taken action based on it. The prohibition on disclosure of PHI also extends to information about whether the patient has paid out-of-pocket to a health plan, unless for treatment purposes or in the event that disclosure is required by law.

B. Business Associates. A business associate relationship exists when an individual or entity acting on behalf of the County assists in creating, receiving, maintaining or transmitting PHI. These services may include legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services. In all cases where there is a business associate relationship, the contract must set forth requirements compliant with 45 CFR 164.504(e), implementing appropriate safeguards to protect the privacy of patient and member information. Business Associates of Covered Entities must be able to demonstrate that they are in compliance with the administrative, physical, and technical safeguards of the HIPAA Security Rule, as part of the American Recovery and Reinvestment Act of 2009 (ARRA).

C. Confidential Communications with Patients and Members. Pursuant to 45 CFR 164.522(b)(i) and (ii), the County may communicate with patients and members regarding test results, appointment reminders, claims, premiums, or items connected with their healthcare or health plan; however, patients and members have the right to confidential communications.

Patients have the right to receive communications regarding their PHI from the County by alternative means or at alternative locations. For instance, if a patient wishes that test results not be left on voicemail or sent to a particular address, the County will accommodate reasonable requests if the individual provides an alternate address or other method of contact. The County will only accommodate reasonable requests.

D. Facility Directory. The County maintains a facility directory for San Mateo Medical Center which lists patients' names, room numbers, general conditions and, if a patient so wishes, religious affiliation. Patients have the right during registration to have their information excluded from the facility directory. Unless a patient affirmatively states that he or she wishes to have his or her personal information excluded from this directory, the information, except religious affiliation, may be disclosed to anyone who requests it by asking for the patient by name. This information, including religious affiliation, may also be provided to clergy members.

E. Family and Friends Involved in Patient or Member Care. The County will disclose limited PHI to designated family, friends, and others who are involved in the patient's or member's care or in payment for such care in the following circumstances:

- i. When the patient is present and has the capacity to make a health decision (i.e. is competent), PHI will be disclosed only if the County obtains the patient's agreement and provides the patient with an opportunity to object to the disclosure

and the patient does not object. Alternatively, in the absence of a verbal objection, the County can reasonably infer that the patient does not object to the disclosure.

- ii. When the patient or member is incompetent, unavailable, incapacitated, or facing an emergency medical situation, PHI will be disclosed only if the County determines, in its professional judgment, that a limited disclosure is in the patient's or member's best interest unless, however, disclosure is preempted by California law. The County may share limited PHI with family and friends without the patient's or member's approval in accordance with 45 CFR 164.510(b)(3).

F. Special Circumstances Disclosure. Unless otherwise preempted by California law, the County may also disclose limited PHI to a public or private entity that is authorized to assist in disaster relief efforts in order for that entity to locate a family member or other persons that may be involved in some aspect of caring for a patient or member.

G. Fundraising. The County may use or disclose to business associates or the "San Mateo County Health Foundation", patient or member demographic information and service dates for its own fundraising purposes in accordance with 45 CFR 164.514(f). Patients have the right to "opt-out" of receiving fundraising materials/communications and may do so by sending their name and address to:

San Mateo Medical Center
C/O Privacy Officer
222 West 39th Avenue
San Mateo, CA 94403

In correspondence requesting exclusion, patients must affirmatively state that they do not wish to receive fundraising materials or communications from the County. The County's *Notice of Privacy Practices* and all fundraising materials must include a statement describing how patients and members can voluntarily opt-out of receiving fundraising communications.

H. Health Products and Services. The County may from time to time use a patient's PHI to communicate with the patient about health products and services necessary for his or her treatment, to advise him or her of new products and services that the County offers, and to provide general health and wellness information.

I. Information Received Pre-enrollment. The County may request and receive PHI from potential members and their healthcare providers prior to enrollment in the health plan. The County will use this information to determine whether an individual is eligible to enroll in the health plan and to determine rates. The County may protect the confidentiality of that information in the same manner as all other PHI it maintains, and if an individual does not enroll

in the health plan the County will not use or disclose the information obtained for any other purpose.

J. Limited Data Set. The County may use PHI to create a limited data set that excludes facially identifiable information that would serve to identify the patient or member or his or her relatives, employers, or household members in accordance with 45 CFR 164.514(e)(2)-(3). The County may use or disclose a limited data set only for the purposes of research, public health or healthcare operations, and only if the County receives a properly executed Data Use Agreement.

The Data Use Agreement must:

- i. Establish permitted uses and disclosures of the limited data set for research purposes;
- ii. Not authorize the recipient to use or further disclose the information in a manner that would violate HIPAA privacy regulations;
- iii. Establish who is permitted to use or receive the limited data set;
- iv. Prohibit use or disclosure of the information other than as provided by the Data Use Agreement or required by law;
- v. Require the recipient to use appropriate safeguards to prevent use or disclosure other than as provided by the Data Use Agreement or required by law;
- vi. Require the recipient to report any use or disclosure not permitted by the Data Use Agreement that the recipient becomes aware of;
- vii. Ensure that any agent or subcontractor of the recipient to whom the limited data set is provided agrees to the same restrictions and conditions set forth in the Data Use Agreement; and
- viii. Require that the recipient not identify the information or contact the individual to whom it belongs in accordance with 45 CFR 164.514(e).

K. Marketing. The County will obtain an authorization for any use or disclosure of PHI for marketing, except when the communication is in the form of:

- i. A face-to-face communication made by the County to a patient; or
- ii. A promotional gift provided by the County pursuant to County Administrative Memorandum B-3. The nominal value of any promotional gift shall not exceed fifty dollars (\$50).

L. Minimum Necessary. When using or disclosing PHI or when requesting PHI from another entity, the County will make reasonable efforts to limit the use and disclosure of PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

M. Permitted Disclosures. The County may release PHI without authorization for any purpose permitted or required by law as set forth in 45 CFR 164.512(a), including to the following parties for the following purposes:

- i. Public health activities;
- ii. Regarding victims of abuse, neglect or domestic violence;
- iii. Health oversight activities;
- iv. Judicial or administrative proceedings;
- v. Law enforcement;
- vi. Regarding deceased persons (including organ and tissue donations);
- vii. Selecting research organizations without any authorization, where permitted by an Institutional Review Board (IRB) or Privacy Board waiver;
- viii. Averting a serious, imminent threat to public safety;
- ix. Specialized government functions (e.g., national security, military, corrections);
- x. Any other purpose as required by law.

N. Psychotherapy Notes. Psychotherapy notes that are considered part of progress notes may be disclosed if an authorization is signed by the patient or the patient's representative, or if the psychotherapy notes are used for one of the following purposes:

- i. By the originator of the psychotherapy notes for treatment;
- ii. By the County's own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling;
- iii. Defense of the County in a legal action or other proceeding brought by a patient;
- iv. To the Secretary of the United States Department of Health and Human Services or his or her designee for compliance investigations;
- v. As required by law;
- vi. To a health agency for oversight of the originator of the notes;

- vii. To coroners and medical examiners; and
- viii. To avert serious threats to health and safety

Psychotherapy notes that are considered process notes and are solely created by and may contain sensitive information relevant to no one other than the provider cannot be disclosed.

O. Research. The County will not use or disclose PHI for research purposes without a patient's or member's authorization unless:

- i. The PHI has been de-identified pursuant to 45 CFR 164.514(a) and thereby does not identify an individual or cannot reasonably be used to identify an individual and is not PHI;
- ii. The PHI is a "limited data set" that excludes certain direct identifiers disclosed and used pursuant to a data use agreement;
- iii. An alteration to or waiver of the authorization requirement in whole or in part is granted by an Institutional Review Board pursuant to federal law;
- iv. The researcher indicates that the PHI is necessary to prepare a research protocol or other similar purpose preparatory to research, the PHI being sought is necessary for research purposes, and that he or she shall not remove any PHI from the County healthcare component that created or maintains the PHI;
- v. As it pertains to research on decedents, the researcher documents the death of the individuals whose PHI is sought, and represents that the use or disclosure of PHI is being sought solely for research and that access to such PHI is necessary for a research purpose in accordance with 45 CFR 164.512(i)(1)(iii).

III. PATIENTS AND MEMBERS RIGHTS

A. Complaints. If patients or members believe their privacy rights have been violated, they may file a complaint by writing to:

San Mateo Medical Center
C/O Privacy Officer
222 West 39th Avenue
San Mateo, CA 94403

In the case of services provided by the Behavioral Health and Recovery Services Division, complaints may be made to the Quality Department at the following address:

Behavioral Health and Recovery Services
225 37th Avenue
San Mateo, CA 94403

The County shall not retaliate against any patient or member who files a complaint and will investigate all formal complaints.

B. Access to Protected Health Information. Patients and members have the right to copy and/or inspect the PHI that the County maintains on their behalf subject to the following:

- i. All requests for access must be made in writing and signed by the patient or member or his or her representative to the respective County Medical Records Department.
- ii. The County must provide access to a patient's or member's records within thirty (30) days of receipt of a written request, unless otherwise preempted by California law. If more time is needed, the County may request an extension of no more than thirty (30) days by notifying the patient or member in writing of the need for more time.
- iii. If requested by the patient, the respective County Medical Records Department will provide a copy of pre-existing electronically stored PHI (ePHI) in electronic format to the patient if the records are readily reproducible in that format. Otherwise, the records shall be provided in another mutually agreeable electronic format. Hard copies are permitted only when the patient rejects all readily reproducible electronic formats.
- iv. The County may charge for individual copies inclusive of labor costs with some exceptions. In the event that California law requires a lower reimbursement rate, copy charges will reflect that rate.

C. Accounting for Disclosures of PHI. Patients and members have the right to receive an accounting of certain disclosures of their PHI made by the County after April 14, 2003, in accordance with 45 CFR 164.528, unless otherwise preempted by California law, and subject to the following:

- i. Requests must be made in writing and signed by the patient, member or his or her representative to the respective County Medical Records Department.
- ii. The first accounting in any 12-month period is provided free of charge. For subsequent requests, patients and members may be charged a fee consistent with the direct cost for each additional accounting requested within the same 12-month period.

D. Amendments to Protected Health Information. Pursuant to 45 CFR 164.526(a), patients and members have the right to request an amendment or correction to their County-maintained PHI. The County is not obligated to make all requested amendments but will give each request careful consideration. All amendment requests, in order to be considered by the County, must be:

- i. in writing; signed by the patient, member or his or her representative; and
- ii. must state the reasons for the amendment/correction request.

The County may deny or grant the amendment request in accordance with 45 CFR 164.526. If the County makes an amendment or correction, the County may also notify others who have copies of the uncorrected version of the patient or member's PHI if the County believes that notification is necessary. Patients and members may obtain an amendment request by contacting the respective County Medical Records Department.

E. Restrictions on Use and Disclosure of PHI. Patients and members also have the right to request restrictions on the use and disclosure of their PHI by the County for treatment, payment, or healthcare operations. Pursuant to 45 CFR 164.522(a)(1)(ii), the County is not required to agree to a patient's or member's restriction request. The County retains the right to terminate an agreed-to restriction if the County believes such termination is appropriate and will notify the patient or member of such termination in accordance with 45 CFR 164.522(a)(2)(iii).

F. No Waiver of Rights. Pursuant to 45 CFR 164.530(h), a workforce member may not require a patient or member to waive any individual rights granted by federal HIPAA regulations as a condition for the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

G. Right to Notice. Patients and members have the right to adequate notice of the uses and disclosures of PHI made by the County as well as his or her rights and the County's legal duties with respect to PHI. Some Health System Divisions such as San Mateo Medical Center (SMMC), Aging and Adult Services and Behavioral Health and Recovery Services (BHRS) have a written Notice of Privacy Practices that is given to patients and members. This Notice of Privacy Practices explains when the County may use and disclose PHI, including in the course of:

- i. Conducting treatment, eliciting or processing payment for treatment or conducting healthcare operations;
- ii. Creation of the facility directory which includes listing the name of the patient, room number, general condition, and, if desired, the patient's religious affiliation;
- iii. Provision of PHI to friends and family involved in the patient's care if the patient provides approval; however, if the patient is unable to provide approval, such PHI

may be shared with those involved in the patient's care if it is determined to be in the best interest of the patient;

- iv. Provision of PHI to outside persons and organizations who assist the County in carrying out services including, but not limited to, auditing, accreditation and legal services;
- v. Fundraising and conducting research;
- vi. Scheduling of appointments and services to provide the patient with services and products specific to his or her care, as well as to advise the patient of new products and to provide general wellness and health information;
- vii. Disclosure of patients' alcohol and drug abuse records. These records are disclosed only if the patient consents to the disclosure, the disclosure is ordered by a court, the disclosure is made in an emergency, or if the disclosure is for a research, audit, or program evaluation; and
- viii. All other uses and disclosures that may be made pursuant to 45 CFR 164.512.

IV. SAFEGUARDS AND HIPAA BREACHES

The County will take reasonable steps to safeguard PHI from any intentional or unintentional use or disclosure that is in violation of the federal HIPAA regulations of patient privacy and confidentiality. The County must reasonably safeguard PHI to limit incidental uses or disclosures made, which are otherwise permitted or required pursuant to the HIPAA privacy regulations. PHI, in whatever form it is stored, shall be subject to safeguard policies and procedures for appropriate categorization, storage, and destruction. The County has developed a retention and destruction policy schedule and copies of a patient's or member's PHI documents are retained for at least a period of seven (7) years.

A. Business Associates and Limited Data Set Users. The County has agreements with business associates who create, receive, maintain or transmit PHI in the provision of services to, and on behalf of, the County, and with limited data set users who use limited amounts of PHI for specified purposes. These agreements include provisions that require the business associate or limited data set user to keep PHI confidential. Per the HIPAA Omnibus Rule published in 2013, see 45 C.F.R. Parts 160 and 164, Business Associates are required to report any PHI breaches directly to the Health and Human Services Office for Civil Rights (OCR), abide by the same rules and regulations as the covered entities they serve, and accept the same penalties. In addition to notification of OCR, Business Associates shall also notify the County of any suspected or reported breach.

B. Breach Analysis

A breach is the acquisition, access, use, or disclosure of PHI in a manner not permitted by applicable law which compromises the security or privacy of the protected health information. A breach is now presumed reportable unless, after completing a risk analysis applying four specific factors, it is determined that there is a low probability of PHI compromise. The County must consider all of the following factors in reaching its decision regarding reporting:

- i. The nature and extent of the PHI involved – issues to be considered include the sensitivity of the information from a financial or clinical perspective and the likelihood that the information can be re-identified;
- ii. The person who obtained the unauthorized access and whether that person has an independent obligation to protect the confidentiality of the information;
- iii. Whether the PHI was actually acquired or accessed, determined after conducting a forensic analysis; and
- iv. The extent to which the risk has been mitigated, such as by obtaining signed confidentiality agreement from the recipient.

C. Mitigating Misuses of Patient Information. Any County workforce member that becomes aware of any misuse of patient or member PHI will immediately notify their supervisor and appropriate personnel in their Division/Department and the County’s Privacy Officer. County workforce members must work with the Privacy Officer to mitigate, to the extent practicable, any harmful effects stemming from the use or disclosure of PHI in violation of this Privacy Policy or any other policy of the County. The County Privacy Officer and/or Department or Division HIPAA Liaisons will report breaches and comply with patient notification standards in accordance with HIPAA, the HITECH Act and California state regulations. See Administrative Memo B-27 for full documentation of the County Protected Health Information Sanction Policy.

V. TRAINING.

The County will train all workforce members carrying out or assisting with covered functions on HIPAA, this Privacy Policy as well as all other PHI-related policies and procedures, as necessary and appropriate and in compliance with 45 CFR 164.530(b) as agreed upon by the County’s HIPAA Oversight Committee. Any workforce members with questions or who may require assistance regarding the County’s privacy practices, should contact:

San Mateo Medical Center
C/O Privacy Officer
222 West 39th Avenue
San Mateo, CA 94403