



Accreditation Standard:
11.1.3.A.1

Not applicable

Policy Number:
20-21

I. PURPOSE:

The purpose of this policy is to ensure that Monterey County Health Department (MCHD) is in compliance with all privacy, confidentiality and security laws; regulations and contractual obligations while utilizing best practices to safeguard the Protected Information (PI) that has been entrusted to the agency by the individuals we serve.

II. DEFINITIONS:

Breach is defined as the acquisition, access, use, or disclosure of unsecured PI in a manner not permitted by the privacy laws applicable to MCHD which compromises the security or privacy of the PI.

Business Associate means a person or entity that, on behalf of the County, acts in a capacity other than a County workforce member to assist the County in carrying out covered functions. For example, these functions could include but are not limited to: performing, or assisting, in a function or activity involving the use or disclosure of Protected Health Information (PHI), including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and re-pricing; or providing or assisting in the performance of legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for the County where the provision of the service involves the disclosure of PHI from the County to the person or entity performing the services.

Compromises the security or privacy: An acquisition, access, use or disclosure of protected health information in a manner not permitted by privacy laws is presumed to be a breach unless the Covered Entity (or Business Associate), demonstrates that there is a low probability that the PI has been compromised based on a risk assessment of at least the following factors:

- Nature and extent of PI involved, including types of identifiers and likelihood of re-identification;
- The unauthorized person who used the PI or to whom the disclosure was made;
- Whether the PI was actually acquired or viewed;
- The extent to which the risk to the PI has been mitigated.

Covered Entity is defined by Health Insurance Portability and Accountability Act (HIPAA) as health plans, health care clearinghouses, and health care providers who electronically transmit any health information in connection with transactions for which Health and Human Services (HHS) has adopted standards.

Covered Functions applies to functions which include but are not limited to healthcare services, health plan services and their respective support services such as: collecting bad 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; legal services; clinical improvement; professional peer review; business management; accreditation and licensing; enrollment; underwriting; reinsurance; compliance; auditing; and rating.

Disclosure means the release, transfer, provision of access to, or divulging in any other manner of PI 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.

ePHI is Protected Health Information in any electronic format.

HIPAA is the federal law Health Insurance Portability and Accountability Act of 1996. It was updated in 2013 as the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, to strengthen the privacy and security protections for health information.

HIV test means any clinical test, laboratory or otherwise, used to identify HIV (human immunodeficiency virus), a component of HIV, or antibodies or antigens to HIV. A diagnosis of AIDS is not considered an HIV test for purposes of the more stringent protections under California law, nor is a patient's self-report of HIV status.

Hybrid Cover Entity: A single legal entity that is a covered entity, performs business activities that include both covered and non-covered functions, and designates its health care components as provided in the Privacy Rule. If a covered entity is a hybrid entity, the Privacy Rule generally applies only to its designated health care components. However, non-health care components of a hybrid entity may be affected because the health care component is limited in how it can share PHI with the non-health care component. The covered entity also retains certain oversight, compliance, and enforcement responsibilities

Personal Identifiable Information (PII): is information directly obtained in the course of performing an administrative function on behalf of MCHD or Medi-Cal that can be used alone, or in conjunction with any other information, to identify a specific individual.

Protected Health Information (PHI): As defined by 45 CFR Parts 160 and 164. Generally, PHI is information that is under the control of MCHD or its Business Associates that relates to the past, present or future condition, either physical or mental, of an individual that would identify that individual, and includes health records and billing records pertaining to healthcare that is provided to a patient. Examples of PHI include but are not limited to:

- Names;
- Street address, city, county, precinct, zip code;
- Dates directly related to a patient or member, including birth date admission date, discharge date, and date of death;
- Telephone numbers, fax numbers, and electronic mail addresses;
- Social Security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;

- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs) and Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code.

Protected Information (PI) is an umbrella term utilized in this policy for PHI, PII, ePHI or other information that is protected under privacy/security laws and regulations that apply to MCHD. PI also includes information that is protected via contractual obligations that MCHD has agreed to comply with.

Safe harbor refers to electronic PHI that has been encrypted as specified in the HIPAA Security rule and follows the National Institute of Standards and Technology (NIST) standards for data at rest and data in motion. In the case of destruction of the media on which PHI is stored, if the media has been destroyed by shredding or such that it cannot be reconstructed or in the case of electronic data, it has been cleared, purged or destroyed according to NIST's Guidelines for Media Sanitation, there is no reporting obligation even if a breach occurs.

Unsecured Protected Health Information means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary of DHHS in the guidance under section 13402(h)(2) of Pub.L. 111-5.

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.

III. DISCUSSION:

It is the policy of MCHD to safeguard the PI of the individuals we serve. This policy requires all staff, including employees, volunteers, interns and students, to comply with all applicable federal and state confidentiality laws, including laws that pertain to the confidentiality and privacy of physical health, mental health, HIV or other sensitive services, and substance use disorder treatment program records. Contract providers are expected to follow all confidentiality laws and all guidelines outlined in this policy, as well as any contractual obligations that may apply.

Related policies include the County of Monterey Security Policies and any additional policies set forth by MCHD and its bureaus that pertain to their work. Managers and Supervisors are required to notify staff of any additional policies at the onset of employment or transfer into the unit and of any changes made to those policies upon implementation.

The Procedure Section is divided into the following sections:

- A. General Confidentiality of PI
- B. Minimum Necessary Rule
- C. Use or Disclosure of PI with Authorization
- D. Patient Access to Records

- E. Confidentiality of HIV Results
- F. PI Away from the Office
- G. Electronic PI
- H. Potential Breach Notification and Investigation Process
- I. Workforce Confidentially Acknowledgements
- J. Other

IV. PROCEDURES:

A. General Confidentiality of PI:

1. Required Disclosures: MCHD staff shall comply with all laws that require the disclosure of PI including requests by individuals to access their own records.
 - a. Child Abuse and Neglect Reporting: When required by law, physical health, mental health and substance use disorder treatment program information may be disclosed to law enforcement and Child Welfare Services in order to report child abuse and neglect. Only that information specifically required by law to be disclosed shall be included in the verbal and written reports. Follow-up information necessary to clarify questions related to what gave rise to suspicion or knowledge of the reported abuse or neglect may be disclosed, but other information concerning the patient or others, for example, close family members, may not be disclosed unless there is authorization from the patient, or a court order.
 - b. Elder and Dependent Adult Abuse and Neglect Reporting: When required by law, physical health and mental health information may be disclosed to law enforcement and Adult Protective Services in order to report elder and dependent adult abuse and neglect. Only that information specifically required by law to be disclosed shall be included in the verbal and written reports. Follow-up information necessary to clarify questions related to what gave rise to suspicion, knowledge, or reported information about the alleged abuse or neglect may be disclosed, but other information concerning the patient or others, for example, close family members, may not be disclosed unless there is authorization or a court order.
 - i. The patient will be notified when an elder/dependent adult abuse and neglect report is made unless to do so would place the patient at risk of serious harm, or it would be mean informing the patient's personal representative (because the patient lacked capacity) and the provider reasonably believes that the patient representative is responsible for the abuse, neglect or other injury and that informing the personal representative would not be in the best interests of the patient.
 - c. Gunshot Wounds and Suspicious Wounds/Injuries: Information must be disclosed to law enforcement when medical care is provided for a physical condition to a patient who appears to have a wound or injury caused by gunshot or by assaultive or abusive conduct.
 - d. For Public Health Reporting: Disclosures are permitted when specifically required by law for public health activities, for reporting births or deaths, and for public health surveillance, investigations or interventions.
 - e. Court Orders, Search Warrants, and Subpoenas: Information must be released to the Court pursuant to a court order or search warrant (signed by a Judge) or to the pursuant to a subpoena properly served with notice to the patient. When providers or staff

- receive such orders they should immediately notify their supervisor or manager so that appropriate steps can be taken to comply with the law.
- f. Coroner: Suspicious deaths must be reported to the Coroner, and additional information may be provided to the Coroner in order to identify a deceased person, determine a cause of death, or other duties authorized by law.
 - g. Secretary of the United States Department of Health and Human Services (US DHHS): All requests for information from the Secretary of the US DHHS should be immediately directed to the attention of the MCHD Privacy Officer. Certain limited disclosures are required when necessary to investigate HIPAA complaints and compliance.
2. Permitted Disclosures: MCHD staff shall comply with all laws that permit the disclosure of PI including requests by individuals that information be disclosed to third parties if it is deemed appropriate by staff.
- a. For Treatment, Payment or Operations: Staff may use or disclose a patient's PHI without an authorization (a) for treatment of the patient, (b) in connection with payment for services provided, or (c) for the County's own internal operations as defined under 45 CFR section 164.501 and permitted under 45 CFR section 164.506 and related state and federal laws.
 - b. With Authorization: Staff may use or disclose a patient's PI with written authorization utilizing an Authorization Form that has been reviewed and approved by the MCHD Privacy Officer.
 - c. With Opportunity to Agree or Object: Information may be disclosed to individual's involved in the patient's care or payment for care if the individual is identified by the patient as someone who is participating in the care or payment and agrees to the disclosure, or when the patient is present and agrees or does not express an objection to the disclosure.
 - d. To Third Parties Without Authorization: Staff may disclose PI without authorization from the patient when otherwise specifically permitted by law, for example to health licensing boards or agencies, for administrative audits or investigations (e.g., CMS audits); to law enforcement to report a crime or threatened crime on the premises, and for approved research. In all of these cases, or where a disclosure is requested and it is not clear whether it is appropriate or permitted, it is important that staff discuss the disclosure with a supervisor or manager, or with the MCHD Privacy/Compliance Officer before the disclosure is made.
 - e. Other Disclosures to Third Parties Not Listed Above: Any other request for information pertaining to a patient, or for copies of records or other materials regarding a person receiving services from MCHD should be directed to the attention of the MCHD Privacy/Compliance Officer. If there is ever any question as to the propriety of disclosing PI to third parties, staff should always check first. If information is disclosed in a manner not required or permitted by all privacy, confidentiality and security laws, regulations and contractual obligations, it will likely require individual notification and breach reporting governing bodies. Fines and penalties are often assessed even in the case of mistaken, non-intentional violations of the law.
 - f. Limited Verbal Disclosures: In certain limited instances, staff is permitted to disclose limited PHI to those involved in the patient's care or treatment when verbally requested or permitted by the patient. For example, the patient may ask staff to tell his girlfriend who is waiting in the waiting room that he will be ready to go in 15

more minutes. Similarly, a patient may ask staff to explain to her daughter where to pick up the patient's recently ordered medication. A simple note in the chart stating that "at the patient's request her daughter was given brief information about picking up her medicine" is sufficient. If a patient asks that more than very limited information be disclosed, it is always best to have a written authorization form completed and signed by the patient.

- g. De-Identified Information: De-identified information may be used or disclosed as long as no means of re-identification is possible. 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.
- h. Limited Data Set: MCHD may use PHI to create a limited data set that excludes facially identifiable information of the patient or member or of relatives, employers, or household members of the patient or member in accordance with 45 CFR 164.514(e)(2)&(3). The MCHD may use or disclose a limited data set only for the purposes of research, public health or healthcare operations, and only if the MCHD receives satisfactory assurances from the recipient of the limited data set in the form of 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 the privacy regulations if done by the County;
 - 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. 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).
 - ix. Be reviewed and approved by the MCHD Privacy/Compliance Officer and County Counsel.

- B. **Minimum Necessary:** Staff will use or disclose only the minimum amount of information necessary to provide services and benefits to individuals, and only to the extent provided in County policies and procedures. Staff will not disclose an entire medical record unless specifically requested by the patient or specific justification is documented. It is the policy of MCHD to ensure that clinicians, employees, students, volunteers and contractors have access to protected health information (PHI) routinely required to accomplish their mission, goals and objectives, but to limit their use and access to PHI to that which is necessary in the course and scope of their work. MCHD will establish role-based categories that identify the type of information necessary for employees, staff and others to do their jobs, and any conditions on use, access or disclosure of PHI. These categories will include access to information that is accessible in paper files as well as that information that is maintained electronically. Access will be monitored and audited on a routine and random basis. Minimum Necessary does not limit use, access or disclosure to and from health care providers or clinicians in the provision of care and treatment to an individual patient, to a patient who seeks access to their own PHI, when disclosures are authorized in writing by the patient, or when specifically required by law. All other disclosures that are permitted by law should be limited to “need to know” or “minimum necessary” guidelines.
- C. **Uses or Disclosures of PI with Authorization:** MCHD staff shall honor requests to use or disclose PI to third parties when requested by the individual and deemed appropriate by staff.
- a. Authorization Form: Whenever feasible the Authorization Form for the specific MCHD program should be used, since it is HIPAA and State law-compliant and staff would not need to further investigate whether the form itself is proper. Authorization forms shall be printed in 14-point type and include an expiration date in order to comply with California Civil Code 56.11. The following core elements shall be included on forms used by MCHD:
 - i. name and date of birth or record number of individual whose records are requested;
 - ii. specific name or general designation of the program or person permitted to make the disclosure;
 - iii. the name or title of the individual or the name of the organization that may use the information or to whom the disclosure is to be made (with address, fax, phone or email address if available);
 - iv. the purpose of the disclosure (either the specific purpose, or if the request is initiated by the individual, it is sufficient to state “at the request of the individual”);
 - v. the information that is to be used or disclosed, described in a specific and meaningful fashion; additionally, if there are any restrictions on the use or disclosure, those should be included;
 - vi. the date on which the authorization will no longer be effective (expiration date);
 - vii. a statement that the authorization is subject to revocation by the individual in writing at any time, except to the extent that the person or program has already acted in reliance on the authorization (specific information on how to do this may be included on the authorization form, or there may be reference to the Notice of Privacy Practices if specific information on where to submit a revocation request is provided there instead);

- viii. the provider's ability or inability to condition treatment, payment, health plan enrollment or eligibility for benefits on the authorization; if the provider will condition services based on signing the authorization, the circumstances in which this kind of limitation is permitted should be described, with an explanation of the consequences of a refusal to sign;
 - ix. the potential for information to be re-disclosed by a recipient who is not required to follow HIPAA or other laws that might otherwise protect the information (e.g., if a disclosure is made to a family member at the request of the patient);
 - x. the rights of the person signing the authorization to receive a copy of the authorization;
 - xi. the signature of the individual or their representative (e.g., a parent or conservator);
 - xii. the date on which the Authorization Form is signed.
 - b. Disclosures Pursuant to a Valid, Signed HIPAA- and State law-compliant Authorization Form: MCHD will ask for a completed and signed HIPAA-compliant Authorization form prior to releasing PHI for determining eligibility in a County administered health plan, to an employer, to school IEP programs, to multi-agency multi-disciplinary teams that include non-clinicians or others not directly involved in providing treatment to the patient, to Social Services in the case of non-mandated disclosures, and to any other third parties, including family members, for which federal or state law requires authorization.
 - c. Prohibition on "Compound" Authorizations: The County will not create or honor authorization forms that have been combined with other documents, such as informed consent, or payment authorization forms.
 - d. Multi-party, Multi-agency Forms. There is no reason why multiple parties cannot be named as recipients, "exchangers" or disclosures of PHI. However, only those named parties intended by the patient and specifically indicated as recipients (or exchangers) of PHI will be provided with information. The patient should indicate (e.g., by check mark or initial) each individual party they intend to include in their Authorization.
 - e. Family Authorizations. When multiple children, or parent and child, etc. are seen as patients, a separate and distinct authorization form is required for each individual patient and each individual sibling.
- D. **Patient Access to Records:** Patients have a right to inspect (access) or receive a copy of their PHI under both Federal and State law. This includes the right to view/access their medical chart and billing records and includes all records maintained by the County, even if the County did not create them (e.g., records sent to the County by another provider). The HIPAA preemption rule provides that the law (or portion of the law) that provides patients with the greatest rights of access should be followed. MCHD notifies patients about this right to access their own (or their child's) record in its Notice of Privacy Practices.
- a. Limitation on the Right to Inspect or Receive Copies of the Patient Record: If access to the record would result in the death of the patient, or in serious physical harm to the patient or someone else, access can be denied to all or part of the record. A decision to deny access is likely to be a rare occurrence, and will be made by the provider in consultation with the MCHD Privacy/Compliance Officer.

- b. When a patient wants to access their own, or their minor child's record, they will be asked to fill out the "Request to Inspect/Copy Record" form that is available from the Records Department of the respective Bureau. The patient does not have to personally deliver the request, and may ask that a copy of the record be mailed to them. Any time there is a request to inspect/copy a record, the provider will be notified that their patient has made this request. If the provider has any hesitation about providing access (i.e., there are concerns about safety of the patient or some other person, or in the case of a parent seeking access to a minor's record, some other concern) the provider should immediately contact the Records Department of the respective bureau, and the MCHD Privacy/Compliance Officer, so that the denial letter can be written. If a denial letter is sent regarding access to all or part of the record, the patient has a right to have the denial reviewed by a licensed health care professional who is designated by the County to act as the reviewing professional and who did not participate in the original decision to deny access.
- c. If the patient wishes to inspect their record, a date and time within five (5) business days will be provided to them to view their record. They may bring one person of their own choosing with them to go over their record with them (Health & Safety Code 123110(a)). Staff will also sit with them as they review their record in order to answer questions, and to insure the integrity of the record is not disrupted. (That is to say, to prevent the removal or destruction or alteration of any of the records.). If the record is an electronic record, staff will assist the patient in accessing their electronic record using MCHD computer equipment, or may provide copies of the electronic record for inspection.
- d. A patient may also request a summary in lieu of a copy of the entire record; MCHD may charge a reasonable fee to provide a summary if it agrees to do that. If the provider does not wish to prepare a summary, the patient will receive a copy of the entire record. If a summary is prepared it must be provided within ten working days unless the patient is notified that more time is needed because of the length of the record, or because the patient was discharged from treatment within the prior 10 days.
- e. If the patient wishes to have a copy of the record sent to them, a copy will be provided or mailed within 15 calendar days of receiving the request.
- f. The patient does not have a right to inspect or obtain copies of information in their record that was provided by someone other than a healthcare provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information. The patient also does not have a right to access information that might be in his or her chart that makes reference to another person where the provider believes that access would be reasonably likely to cause substantial harm to that person. The patient does not have a right to access or inspect or get copies of their mental health professional's private notes written down during a counseling session that are separated from the rest of the record and are merely relied on by the professional after the counseling session to write his or her progress note in the chart. These so-called "psychotherapy notes" that are not accessible to the patient, do not include the following information to which the patient would have access: information about medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date (45 CFR 164.501 – Definitions:

Psychotherapy notes). There are other exceptions that the MCHD Privacy/Compliance Officer can be consulted on if the need arises (e.g., access to records used in research, related to care provided in correctional settings, or that may be exempt under other laws).

- g. Generally, the patient representative (parent, legal guardian, conservator, agent, etc.) has the same right to access the record as the patient would have. However, access may be limited if the provider believes that it would likely cause substantial harm to the individual or some other person. In this situation the MCHD Privacy/Compliance Officer should be consulted. In the case of parents wishing to access the record of a minor child, that request must be denied if the minor could have, or did consent to their own care under minor consent law as an emancipated or self-sufficient minor, or because they qualify under "sensitive services" exceptions. In those cases, the minor must authorize disclosure to their parent, per third party authorization process. If the minor could not have consented to their own care, the parent or legal guardian can still be denied if the provider believes that access to all (or part) of the record will have a detrimental effect on the provider's professional relationship with the minor patient or the minor's physical safety or psychological well-being. In this situation the MCHD Privacy/Compliance Officer should be consulted.
- h. MCHD may charge the patient a reasonable cost-based fee to provide access, write a summary, or provide copies of the electronic or paper record. The copying cost may not exceed \$0.25/page (\$0.50 for copies from microfilm), or reasonable costs for copying x-rays or tracings from various equipment. Also, the patient may be asked to pay reasonable administrative fees that may include the staff time it takes for copying, summarizing, compiling, extracting, scanning, or collating the material. Postage costs may also be charged. The costs may not include the time spent locating the record. Fees may be collected prior to the provision of copies and access, but access cannot be conditioned on the payment of unpaid bills for health care services themselves. A patient does not have to pay a fee if the records are needed in an appeal regarding eligibility for Medi-Cal, Social Security disability insurance benefits, or SSI/SSP benefits. If the appeal is successful, MCHD may later bill the patient for the fees. The patient is entitled to just one free set of records pursuant to this provision of the law, and the copies must be provided within 30 days. If the patient is represented by a private attorney who is paying for the costs related to the appeal pending its outcome, the patient is not entitled to the free copy.

E. **Confidentiality of HIV Test Results:** It is the policy of MCHD to protect the use and disclosure of HIV test results and strictly limit the disclosure of those results if they are included in any records of any patient of MCHD. The results of an HIV (human immunodeficiency virus) test are confidential and subject to all of MCHD policies that protect the use and disclosure of patients' PHI regardless of where the results of an HIV test are kept. Additionally, California law provides for stricter privacy limits that specifically apply to HIV test results and how they may be used and disclosed.

- a. **Maintenance of Test Results in Record:** When HIV test results are recorded in a MCHD record, they should be placed in section where all other laboratory results are kept. They should not be hidden in the back of the chart, nor should the record be specially marked in any manner that would indicate specifically that HIV test results are part of the chart. However, the chart should be discreetly flagged to indicate that it contains

information that may require special treatment prior to disclosure to anyone who is not on the treatment team or providing direct treatment services to the patient.

- b. An entry in the patient record about an HIV test, or containing the results of an HIV test, is not considered to be a “disclosure” of the test results and therefore does not require written authorization from the patient prior to placing that information in the patient record. Treatment providers and their agents or employees who provide direct patient care and treatment to a patient are authorized by law to have access to test results or information about the HIV test that may be included in the patient’s record without the need for written authorization.
 - c. Release of HIV Test Results or Record Containing Those Results: If the chart is flagged (electronically or through some other means) to indicate that it contains confidential information that may require special treatment, for example HIV test results or substance use disorder treatment program information, the Records Room Technician must limit disclosure or release, transmission, dissemination, or communication whether orally, in writing or by electronic transmission until appropriate steps are taken to protect that information. If HIV test results are included in the health record, the patient’s authorization that specifically includes permission to disclose HIV test results must be obtained before the part of the records that include the test results are disclosed to third parties, in response to a subpoena, or for other reasons not specifically permitted or required by law. The Records Room Technician should consult with the MCHD Privacy/Compliance Officer if other disclosures of HIV test results are requested and authorization has not been obtained, e.g., for workplace exposures to bloodborne pathogens or Court orders involving certain criminal defendants.
 - d. The general healthcare provider who ordered the HIV test typically handles disclosures to the public health authority, or to specialty care providers.
- F. **PI Away from the Office:** It is the policy of MCHD to limit the removal of PI from any MCHD facility unless absolutely necessary in order to provide services to our clients. In those cases where staff must transport or carry PI away from an MCHD facilities, they must take steps to assure that the information is limited to the minimum necessary to accomplish the task at hand, and that appropriate administrative, technical and physical safeguards are employed to reduce the risk of a breach of privacy. No staff will be permitted to take, copy, or create PI to carry with them to an off-site location unless permitted to do so by their supervisor and by MCHD policy. If any of the paperwork, written information, client chart, or any electronic device with PI on it is lost, misplaced or stolen, a breach report must be filed with the MCHD Privacy/Compliance Officer *immediately* so that a proper investigation can be conducted, and if necessary, the patient can be notified and the breach reported. Prior to removing PI from the safety and security of a County office or facility, staff shall take Administrative, Physical and Technical Safeguards to protect the PI.
- a. Administrative Safeguards:
 - i. Staff must assure that the creation, use or transport of PI away from their office or facility is necessary to their job and no reasonable alternatives exist.
 - ii. Staff should confirm that MCHD policy and their supervisor permits the creation, use or transport of the PI away from the office or facility in the manner proposed, and the supervisor is aware that this staff person is engaged in this practice.

- iii. Staff must assure that only the “minimum necessary” information is taken, and that no identifying information is included with the PI that is extraneous or unnecessary to the task at hand. De-identification of as much of the PI as is feasible should be done prior to removing it from the office or facility; for example, if a page from the chart will suffice, only that page should be copied and taken. Similarly, if the client’s name, address and phone number are needed for a field case worker to contact and meet with the client, the client’s birth date and social security number should not be included with the “paperwork” that leaves the office or facility; if initials or first name/last initial or vice versa suffices, full names should not be used.
 - iv. After the visit or task is finished, the PI should be promptly returned to the office or facility and stored securely; or, if it is not part of the designated record set and is no longer needed (for example, a brief list of client names and addresses to be seen that day) it should be placed in the blue shred bins (or destroyed as the program requires).
- b. Physical Safeguards:
- i. Any paper documents containing PI should be kept with staff at all times. PI should not be left on a table, in an office, or in any private or public place where it is not constantly within sight and control of staff.
 - ii. If documents cannot be returned the same day that they are removed from the office or facility, they should be kept with staff inside their home rather than in a locked vehicle. Staff must not allow unauthorized household members to view the documents.
 - iii. If documents must be kept in a locked vehicle, for example while other clients are seen in their homes, they should be kept in the locked glove box or trunk of the car, or otherwise covered or kept out of sight, so that it is not apparent that PI or other confidential information is in the car.
- c. Technical Safeguards: View the following Monterey County Information Technology policies at: <http://www.in.co.monterey.ca.us/infosec/>: Briefly, the following steps must be taken:
- i. If PI is on a laptop computer or other electronic device such as a phone, the device must be password protected and PI stored on it should be encrypted.
 - ii. Personal electronic devices should not be used to store PI and any PI that is temporarily on such a device should be promptly removed/deleted.
 - iii. Personal electronic devices should be equipped with lost device “wiping capability” so that if the device is lost, misplaced or stolen, the data on it can be remotely erased. The employee should be aware that they may lose personal information if the device must be wiped before they accept a personal device stipend.

G. **Potential Breach Notification and Investigation Process:** It is the policy of MCHD and its contracted providers to notify individuals of privacy/security breaches of PI. In compliance with the terms of its contracts with the California (CA) Department of Health Care Services (DHCS), MCHD will report all breaches of PI to CA DHCS. In addition, MCHD will report those same breaches to the Secretary of the Department of Health and Human Services (DHHS) as mandated by the Health Information Technology for Economic and Clinical Health Act (HITECH Act), Title XIII of Division A of the American Reinvestment and Recovery Act of 2009 (ARRA) and the regulations

found in the Final Rule published January 25, 2013 in the Federal Register (78 Fed. Reg.5566), Effective Date: March 26, 2013, and Compliance Date: September 23, 2013. The policies and procedures described herein apply retroactively to breaches that occurred on or after September 23, 2009, and to all breaches, as defined, that occur while this policy is in effect. See the definitions above for Breach.

- a. See the definitions above for Breach. Exceptions to the term “breach” include:
 - i. Unintentional acquisition, access, or use of PI by a workforce member or person acting under the authority of a covered entity (CE) or business associate (BA) if the acquisition, access, or use was made in good faith and within the course and scope of the authority and does not result in further use or disclosure in a manner not permitted by the Privacy Rule (ex: opening the wrong record because two patients have similar names).
 - ii. Any inadvertent disclosure by a person who is authorized to access PI at a CE or BA to another person authorized to access PI at the same CE or BA, or organized health care arrangement (OHCA) in which the CE participates, and the information received is not further used or disclosed in a manner not permitted by the Privacy Rule (a fax is sent to another medical provider and it has been recovered or destroyed- contact the MCHD Privacy/Compliance Officer for documentation requirements).
 - iii. A disclosure of PI where a CE or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information, for example, sending PI in the mail to the wrong address where the mail is returned unopened to the post office as undeliverable, or where a nurse mistakenly hands discharge papers to the wrong patient, quickly realizes the mistake, and recovers the PI before the patient has time to read it.
- b. When there is suspicion of a breach: Any employee, volunteer, student, agent, contractor, business associate or other person or entity working on behalf of this facility who suspects that there may have been an acquisition, access, use, or disclosure of unsecured PI in a manner not permitted by this shall **immediately** notify their supervisor and the MCHD Privacy/Compliance Officer (or their designee). The Privacy/Compliance Officer can be contacted at (831) 755-4522 or 411Privacy@co.monterey.ca.us. A Special or Unusual Incident Form must be submitted within 48 hours ([Privacy Forms](#)).
- c. Assessment of the breach: An assessment will be done in the case of every potential reportable breach to determine whether it meets one of the three exceptions listed in the definitions section of this policy or that based upon a risk assessment, it is determined that there is a low probability that the PI has been compromised. The decision to notify the individual and report the breach will be role of the MCHD Privacy/Compliance Officer and County Counsel.
- d. Breach Risk Assessment: All risk assessment will be conducted by the MCHD Privacy/Compliance Officer and/or County Counsel. Notification and reporting is not required if it is determined that there is a low probability that the PI has been compromised. All risk assessments and written documentation must be retained for at least six (6) years. If it is determined that there was a breach, the individual must be notified and the breach must be reported to any and all agencies that pertain to the

breach. When doing the risk assessment as to whether the PI has actually been compromised, staff conducting the assessment shall address the following issues:

- i. The nature and extent of PI involved, including the types of identifiers and likelihood of re-identification (for example, if only a persons' first initial and last name was released, with no other information on a list vs. an individual's name, date of birth, and social security number, or a patient's HIV, mental health or substance abuse treatment information).
 - ii. The unauthorized person who used the PI or to whom the disclosure was made (for example, if the recipient also must comply with federal privacy laws because it is a federal agency or is itself a CE)
 - iii. Whether the PI was actually acquired or viewed (for example, if IT specialists assure through their investigation that patient data on a stolen laptop was never accessed).
 - iv. The extent to which the risk to the PI has been mitigated (for example, For example, did the recipient provide satisfactory assurances that the PI will not be further disclosed, was not read, and has been destroyed?)
- e. Notification must be made without reasonable delay and no later than sixty (60) days after discovery. A breach is deemed discovered when an employee, officer, or other agent of MCHD or BA other than the individual committing the breach, knew or should reasonably have known about the breach. If law enforcement asks to delay notification/reporting because it would impede a criminal investigation or cause damage to national security, then notification shall be delayed as advised by County Counsel.
- f. Notification should be by first class mail to the individual's last known address, unless the individual has specified a preference for email or other means. If the individual lacks capacity, MCHD will notify the personal representative (e.g., parent of a minor). If the individual is deceased, MCHD notify the next of kin. If notification is urgent because of possible imminent misuse of the unsecured PI, notification of individuals will be conducted by phone or other means as appropriate; additionally, written notification is still required. Notification will be conducted by the MCHD Privacy/Compliance Officer or their designee.
- g. If fewer than ten patients cannot be reached by first class mail, then substituted means of communication should be employed. This may involve phone calls, website notification, or use of the media, whichever is most likely to reach the individuals. If there are ten or more individuals for whom there is insufficient or out-of-date contact information, then one of the following is required. Either method requires a minimum posting of 90 days and a toll free number that an individual can call to find out if his/her unsecured PI was included in the breach.
- i. a conspicuous posting on the MCHD home page of our website
 - ii. notice in major print or broadcast media (including major media where individuals likely reside)
- h. When notifying individuals by any method, the following information should be included in the notice that is provided:
- i. Brief description of what happened
 - ii. Date of the breach, if known
 - iii. Date of discovery of the breach

- iv. Description of types of information involved such as full name, date of birth, home address, account number, disability code, etc.
 - v. Steps that individual should take to protect him/herself from potential harm resulting from the breach
 - vi. Brief description of what MCHD is doing to investigate the breach, mitigate losses and protect against further breaches
 - vii. Contact procedures for individuals who have questions, which must include a phone number, email address, website or postal address
- i. If there is a breach of unsecured PI of 500 or more residents of a state or jurisdiction, notice must also be provided to prominent media outlets serving that state or jurisdiction, in addition to written notice to each individual.
 - j. MCHD (or BA, if BA agreement requires it) must be able to demonstrate that all notifications were made as required (or that a use or disclosure did not constitute a breach because there was no potential risk of harm), thus written documentation will be retained for at least six (6) years.
 - k. **Mandatory Reporting:** In accordance with the terms of MCHD's contracts, California Department of Health Care Services (CA DHCS) must be notified of all reportable breaches. MCHD will comply with the reporting standards and procedures set out in the terms of its current contract with CA DHCS. The Secretary of the Department of Health and Human Services (DHHS) must also be notified of all reportable breaches. In situations where 500 or more individuals are involved in a single breach, the notice must be provided immediately. If fewer than 500 individuals are involved, MCHD may maintain a log or other documentation which must be submitted annually to the DHHS. This log or other documentation must be provided within 60 days after the end of the calendar year in which the breach was discovered (March 1 most years, Feb 29 in leap years).
 - l. Upon discovery of a reportable breach, Business Associate (BA) has the same notification and reporting obligations as MCHD. It all BA Agreements must include provisions that the BA must notify MCHD without unreasonable delay after discovery of the breach. Notice to MCHD must include, to extent possible, the identification of individuals whose PI was breached and all other available information that is listed above as information that MCHD must provide in any notice to the individual; information that becomes available later should also be provided to MCHD. If BA is acting as an agent, then the time to notify the individual runs from the time of the breach, not from the time the MCHD learns of it. If BA is an independent contractor, then notification time is based on the time MCHD is first notified of the breach. The BA contract may specify whose responsibility it will be to provide notifications (individuals should not receive two notices because duplicate notices about the same breach could be confusing).
- H. **Workforce Confidentially Acknowledgements:** MCHD has a duty to implement reasonable measures to maintain an adequate level of privacy and security of all PI that it creates, maintains and stores. All staff, employees, contractors, volunteers, consultants and students who work either directly or indirectly with MCHD PI will not be granted access to MCHD PI unless and until they sign the MCHD Confidentiality and Non-Disclosure Acknowledgement. This policy is not intended, and should not be construed, to limit, prevent, or prohibit employees from complying with or exercising their rights under any applicable federal state, or local law.

- a. MCHD shall train all staff, employees, contractors, volunteers, consultants and students who work with PHI about MCHD's policies or procedures to safeguard PHI annually. Individuals will have the opportunity to ask question to clarify their understanding of policies and procedures.
- b. Only authorized individuals and users are granted access to PI. Such access is limited to specific, defined, documented and approved purposes, and level of access rights. Such access is also limited by the HIPAA minimum necessary rule.
- c. As a condition to receiving access rights to MCHD PI (either electronic or hard copy access), every employee and other user must agree, in writing, to comply with established terms and conditions MCHD Confidentiality and Non-Disclosure Acknowledgement. Failure to comply with such terms and conditions may result in the denial and/or immediate suspension of access to PI and considered a violation of this policy to be referenced to Human Resources for further review.
- d. A violation of the terms of the MCHD Confidentiality and Non-Disclosure Acknowledgement agreement may be grounds for disciplinary action, including termination of employment or contract, loss of privileges, legal action for monetary damages, and other civil and criminal fines and penalties that may apply.
- e. MCHD Confidentiality and Non-Disclosure Acknowledgement shall be signed annually by each employee. Copies should be retained by the employee and their direct supervisor. The original signed copy shall be stored in the Employee Record that is kept by Human Resources.

I. Other:

- a. Fundraising, Marketing, and Sale of PI: Under no circumstances will PI be used for fundraising, marketing or sale without specific action by Administration and approval of the MCHD Privacy/Compliance Officer.
- b. Media and Other Inquiries: All media inquiries involving PI should be referred immediately to the MCHD Privacy/Compliance Officer for review.
- c. Minors: Use and disclosure of PI associated with minors should be administered using the same principles as consent for treatment or services as such case management. If the minor can consent for services per federal or state statute or MCHD policy, then the minor controls his or her privacy rights.
- d. Research: MCHD will not use or disclose PI for research purposes without a patient or member's authorization meeting the requirements of 45 CFR 164.508 unless:
 - i. PHI has been de-identified pursuant to 45 CFR 164-514(a);
 - ii. The PHI is a "limited data set" disclosed and used pursuant to a data use agreement meeting the requirements of 45 CFR 164.514(e);
 - iii. An alteration to or waiver of the authorization in whole or in part is granted by an Institutional Review Board pursuant to federal law and documented in accordance with 45 CFR 164.512(i)(2);
 - iv. The PHI is necessary to prepare a research protocol or other similar purpose preparatory to research, where the PHI being sought is necessary for research purposes, and the researcher does not remove any PHI from the MCHD healthcare component that created or maintains the PHI in accordance with 45 CFR 164.512(i)(1)(ii);
 - v. The researcher documents the death of the individuals whose PHI is sought, and represents that the use or disclosure is being sought solely for research on the

PHI of decedents and that access to such PHI is necessary for a research purpose in accordance with 45 CFR 164.512(i)(1)(iii).

- vi. PII or other PI must be approved for use by the MCHD Privacy/Compliance Officer before disclosure and for the need of a registered institutional review board (IRB) analysis.
- e. Encrypting emails: Emails including Social Security numbers must always be encrypted. PI should not be sent in unencrypted email. PI should be kept within the secure systems designed for their utilization (i.e.: Electronic Medical Records, Lab Data Management Systems, and Client Management Systems). When working with partners who are not allowed access to these systems, the PI should be de-identified before it is emailed (i.e. "patient 12345 is being moved to site B from site A. Please transfer billing to site B"). Any additional information must be encrypted or faxed via a confirmed and confidential fax line.

V. REFERENCES:

- A. General Confidentiality of PHI:
 - 45 CFR Subpart B, Sections 160.201 et seq. (HIPAA: Preemption of State Law)
 - 45 CFR 164.506, 164.508, 164.510, 164.512
 - California Civil Code 56.10 et seq.
 - California Health and Safety Code 120980, 121010
- B. Minimum Necessary Rule:
 - 45 CFR Parts 160 and 164
 - 45 CFR 164.502
- C. Use or Disclosure of PHI with Authorization:
 - 45 CFR Subpart B, Sections 160.201 et seq. (HIPAA: Preemption of State Law)
 - 45 CFR 164.508 (HIPAA: Disclosures with Authorization)
 - California Civil Code 56.10 and 56.11
 - California Health and Safety Code 120980, 121010
 - California Welfare and Institutions Code 5328
- D. Patient Access to Records:
 - 45 CFR Subpart B, Sections 160.201 et seq. (HIPAA: Preemption of State Law)
 - 45 CFR 164.524 (HIPAA: Access of individuals to protected health information);
 - California Health and Safety Code 123100-123149.5 (Patient Access to Health Records Act)
- E. Confidentiality of HIV Results:
 - 45 CFR Parts 160 and 164
 - Civil Code 56.10 et seq.
 - Health and Safety Code 120980 and 120985
- F. PI Away from the Office:
 - 45 CFR Parts 160 and 164
- G. Potential Breach Notification and Investigation Process:
 - 45 CFR Parts 160 and 164
- H. Workforce Confidentiality Acknowledgements:
- I. Other:
 - 45 CFR Part 164.312(e)(1)

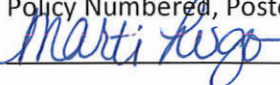

VI. ORIGINATOR:

Molly Hubbard, MS
Privacy/Compliance Officer
Administration Bureau
831-755-4522
hubbardmc@co.monterey.ca.us

Appendix A: Signature Page

Originator: Molly Hubbard, Privacy/Compliance Officer, Administration Accreditation Requirement 11.1.3.A.1	Frequency of Review: Annual
Approved by: Executive Team	

Approved and signed:  _____ Ray Bullick, Director		Date: 11/13/15
--	---	------------------------------

Policy Numbered, Posted, and Distributed  _____		Date: 11/13/2015
--	---	--------------------------------

Revisions:

<i>Author</i>	<i>Revised Section</i>	<i>Revision #</i>	<i>Date Released</i>

Always refer to <http://sharepoint/sites/mchd/HPP/Forms/AllItems.aspx> for the current controlled version