Monterey County Behavioral Health
Policy and Procedure

Policy Number	322
Policy Title	Protected Health Information (PHI) Breach Notification and Mandatory Reporting
References	• Health Insurance Portability and Accountability Act • Health Information Technology for Economic and Clinical Health Act (HITECH Act), Title XIII of Division A of the American Reinvestment and Recover Act of 2009 (ARRA)
Form	Attachment 1: PHI Breach Reporting Procedures Attachment 2: Monterey County Behavioral Health Quality Improvement Breach Assessment and follow up procedures Attachment 3: Monterey County Health Department Special an
Effective	January 16, 2014 **REVISED**: April 24, 2014

Policy

Policy: It is the policy of Monterey County Behavioral Health (MCBH) and its contracted providers to notify individuals (beneficiaries) of privacy/security breaches of protected health information (PHI). In compliance with the terms of its contract with the California (CA) Department of Health Care Services (DHCS), MCBH will report all breaches of PHI to CA DHCS. In addition, MCBH 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.

Effective Date of This Policy: 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.

Definitions:

- "Breach" is defined as the acquisition, access, use, or disclosure of "unsecured" PHI in a manner not permitted by the Health Insurance and Portability and Accountability Act (HIPAA) Privacy Rule which compromises the security or privacy of the PHI.

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

    1. Nature and extent of PHI involved, including types of identifiers and likelihood of re-identification;

    2. The unauthorized person who used the PHI or to whom the disclosure was made;

    3. Whether the PHI was actually acquired or viewed;

    4. The extent to which the risk to the PHI has been mitigated.

- "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.

- Exceptions: the term “breach” does NOT include:

    1. Unintentional acquisition, access, or use of PHI 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.

    2. Any inadvertent disclosure by a person who is authorized to access PHI at a CE or BA to another person authorized to access PHI 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.

3. A disclosure of PHI 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 PHI 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 PHI before the patient has time to read it.

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” PHI in a manner not permitted by the Privacy Rule shall immediately notify their supervisor and the MCBH Quality Improvement (QI) Team. The QI Team can be contacted at (831) 755-4545. The QI Team will then immediately notify the Monterey County Health Department (Health Department) Privacy Officer and consult with Monterey County Counsel (County Counsel) regarding the situation.

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 PHI has been compromised. If the decision is made to notify the patient and report the breach regardless of the outcome of the assessment, an assessment need not be made. The decision to notify the patient and report the breach must be done in consultation with the MCBH QI Team, Health Department Privacy Office, and County Counsel.

If it is determined that it meets an exception, or that there is a low probability that the PHI has been compromised based upon at least the four factors that must be considered in the assessment as described above, the person making that determination shall prepare written documentation of that determination and submit it to the MCBH QI Team, who will retain it for at least six (6) years. The MCBH QI Team will then send the written documentation to the Health Department Privacy Officer and to County Counsel for review. Patient notification and reporting to the DHHS is not required in the case of an exception or determination that there is a low probability that the PHI has been compromised.

Breach Risk Assessment

Note: *A HIPAA breach risk assessment tool is available through MCBH QI to assist in completing the necessary breach risk assessment. Contact MCBH QI at*

831-755-4545 for additional information regarding the breach risk assessment tool.

All risk assessment will be conducted by QI Team clinical staff, the Health Department Privacy Officer, and/or County Counsel. When doing the risk assessment as to whether the PHI has actually been compromised, staff conducting the assessment shall address the following issues:

1. Nature and extent of PHI involved, including types of identifiers and likelihood of re-identification (for example, if only a patient's first initial and last name was released, with no other information on a list vs. a patient's name, date of birth, and social security number, or a patient's HIV, mental health or substance abuse treatment information)

2. The unauthorized person who used the PHI 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)

3. Whether the PHI was actually acquired or viewed (for example, if IT specialists assure through their investigation that patient data on a stolen laptop was never accessed)

4. The extent to which the risk to the PHI has been mitigated (for example, For example, did the recipient provide satisfactory assurances that the PHI will not be further disclosed, was not read, and has been destroyed?)

Notification and reporting is not required if it is determined that there is a low probability that the PHI has been compromised. However, the risk assessment and written documentation determination must be retained for at least six (6) years.

If it is determined that there was a breach, the patient must be notified and the breach must be reported to the DHHS.

Breach Notification to Individual whose PHI was Breached

When: Notification must be made w/o reasonable delay and no later than sixty (60) days after discovery. A breach is deemed discovered when an employee, officer, or other agent of the covered entity or business associate other than the individual committing the breach, knew or should reasonably have known about the breach.

Law Enforcement Exception: if law enforcement asks you to delay notification/reporting because it would impede a criminal investigation or cause damage to national security, then you should delay notification/reporting until the investigation is completed. If the request is made orally, you should document

the statement, identify the law enforcement agency or official making the statement, and temporarily refrain from notification or reporting, but no longer than 30 days, unless a written statement is submitted during that time.

How: 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 patient lacks capacity, notify the personal representative (e.g., parent of a minor). If the patient is deceased, notify the next of kin.

If notification is urgent because of possible imminent misuse of the unsecured PHI, you should notify individuals by phone or other means as appropriate; additionally, written notification is still required.

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.

Breach involving 10 or more patients who cannot be reached: 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:

- a conspicuous posting on the covered entity's home page of their website, OR

- notice in major print or broadcast media (including major media where individuals likely reside)

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 PHI was included in the breach.

Content of notice to individuals: When notifying individuals by any method, the following information should be included in the notice that is provided:

- Brief description of what happened
- Date of the breach, if known
- Date of discovery of the breach
- Description of types of information involved such as full name, date of birth, home address, account number, disability code, etc.
- Steps that individual should take to protect him/herself from potential harm resulting from the breach
- Brief description of what the CE is doing to investigate the breach, mitigate losses and protect against further breaches
- Contact procedures for individuals who have questions, which must include a toll-free number, email address, website or postal address.

Large Breaches (500+): If there is a breach of unsecured PHI 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.

Documentation of Notification: The CE (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), so it is essential that written documentation be retained for at least six (6) years.

Mandatory Reporting to CA DHCS:

In accordance with the terms of MCBH's contract, CA DHCS must be notified of all reportable breaches. MCBH will comply with the reporting standards and procedures set out in the terms of its current contract with CA DHCS.

Mandatory Reporting to DHHS:

The Secretary of the DHHS must 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, the CE 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).

DHHS Reporting Form: A form has been developed that may be completed online that is titled
Notice to the Secretary of HHS of Breach of Unsecured Protected Health Information (OMB Form No. 0990-0346). It can be found at www.dhhs.gov (search terms: "notice of breach").

Breaches by Business Associates

Upon discovery of a reportable breach, BA has the same notification and reporting obligations as the Covered Entity. It is recommended that all BA Agreements include provisions that the BA must notify CE without unreasonable delay after discovery of the breach.

Notice to the CE must include, to extent possible, the identification of individuals whose PHI was breached and all other available information that is listed above as information that the CE must provide in any notice to the individual; information that becomes available later should also be provided to CE.

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 CE learns of it. If BA is an independent contractor, then notification time is based on the time CE 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).

Note: The CE or BA is not responsible for a breach by a third party to whom it permissibly disclosed PHI unless the third party is an agent of the BA or CE.

Attachment 1: Protected Health Information Breach Reporting Procedures

Steps to be taken:

- ☐ The MCBH staff or contract provider directly involved in the incident and/or their supervisor/manager will call MCBH QI at 831-755-4545 and provide a verbal report of the suspected PHI breach to a member of the MCBH QI clinical team
- ☐ **NOTE:** ***The verbal report to MCBH QI must be done in the same day as the discovery of the potential breach!***
    - For the verbal report to QI, be ready with specific information regarding the suspected PHI breach, including a list of clients possibly affected
    - If after hours, leave a message on the confidential MCBH QI voicemail regarding the suspected breach and a clinical staff member will contact you the following business day. Leave the following information in the voicemail:
        - Name
        - Team, program, or agency name
        - Contact number
        - Supervisor or program manager name
        - Supervisor or program manager contact number
- ☐ Complete the Monterey County Health Department Unusual or Special Incident Report per MCBH Policy 123 – Unusual Incident Reporting
    - Unusual or Special Incident Report needs to include, at minimum, detailed information regarding the following:
        - Circumstances of the suspected breach
        - Location (including full address) of suspected breach
        - A list of client IDs whose PHI is involved in the suspected l breach
        - A detailed description of the PHI possibly impacted by the suspected breach. The information should contain but not be limited to the following:
          NOTE: *This is extremely critical information as the type of PHI affected determines the level of mitigation and correction MCBH needs to engage in*
        - What type of media was the PHI contained in (e.g., electronic, paper)?
        - What type of PHI was potentially breached (e.g., client IDs, names, social security numbers)?
        - How was the PHI stored (e.g., Was the PHI a list of client IDs or client names? Was this list placed with a calendar with client names and appointments? Was the staff's MCBH business card attached or near?
    - Fax completed report to the following:
        - MCBH QI – Fax: 831-755-4350
        - MCBH Administration – Fax: 831-755-4980
- ☐ Please have reporting staff and supervisor(s)/manager(s) prepared for follow up questions and inquiries from MCBH QI.

Attachment 2: QI Breach Assessment and Reporting Procedures

NOTE: The following procedures are for the ***Quality Improvement Team ONLY***

I. Inform County Counsel and Health Department Privacy Officer via email of potential PHI breach

- ☐ QI clinical staff will complete California Department of Health Care Services (DHCS) Privacy Incident Reporting Form ("PIR") located at http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/CountiesOnly.aspx with as much information as possible
- ☐ QI will send PIR to County Counsel and Health Department Privacy Officer for review with clear indication that reply is needed ASAP in order to comply with DHCS timelines (*within 72 calendar hours*)
    - County Counsel staff to be notified:
        - Stacy Saetta
        - Anne Brererton
    - Health Department Privacy Officer to be notified:
        - Molly Hubbard
- ☐ Cc: Amie Miller, MCBH QI Services Manager

II. Notify the California Department of Health Care Services ("DHCS") of potential PHI breach as soon as County Counsel and Health Department Privacy Officer replies regarding initial PIR

- ☐ Once County Counsel and Health Department Privacy Officer replies, QI will forward PIR via email to DHCS contract monitor, privacy officer, and information security officer
    - DHCS contacts to be informed:
        - Contract monitor: Erika.Cristo@ca.dhcs.gov (*NOTE: check on a regular basis if this remains the DHCS contract monitor for MCBH*)
        - DHCS Privacy Officer: privacyofficer@ca.dhcs.gov
        - DHCS Information Security Officer: iso@ca.dhcs.gov
- ☐ Cc: MCBH QI Services Manager
- ☐ Cc: Health Department Privacy Officer

III. Conduct PHI breach assessment and develop strategies to mitigate harm

- ☐ QI clinical staff will gather additional information regarding the incident and compile gathered information in MCBH Potential HIPAA Breach Investigation and Assessment Information form
- ☐ QI clinical staff will utilize the California Hospital Association (6/13) HIPAA Breach Decision Tool and Risk Assessment Documentation Form to determine if the reported incident was an actual PHI breach and assess the risk level of the breach
- ☐ If the HIPAA Breach Decision Tool and Risk Assessment Documentation Form indicates that a breach occurred, QI staff will develop risk mitigation plan, corrective action plan, and client notification plan (in compliance with standards provided by DHCS)
- ☐ QI clinical staff will update DHCS PIR form with relevant information from the MCBH Potential HIPAA Breach Investigation and Assessment Information and the HIPAA Breach Decision Tool and Risk Assessment Documentation forms
    - o List of affected client IDs does not need to be transferred to DHCS PIR
    - o Privileged communications between County Counsel and QI should not be entered into DHCS PIR
- ☐ QI clinical staff will submit the updated DHCS PIR form along with notification plan (including general versions of beneficiary notification letters) for review to:
    - o County Counsel
    - o Risk management consultant (if available), and
    - o Health Department Privacy Officer
- ☐ Cc: MCBH QI Services Manager

IV. Submit an updated PIR to DHCS within the specified time line (*10 working days)*

- ☐ Make changes to DHCS PIR requested by County Counsel, risk management consultant (if available), and Health Department Privacy Officer
- ☐ Once changes are made to DHCS PIR, QI will forward PIR via email DHCS contract monitor, DHCS Privacy Officer, and DHCS Information Security Officer
- ☐ Cc: MCBH QI Services Manager
- ☐ Cc: Health Department Privacy Officer

V. Follow through on risk mitigation, correction action, and client notification plans

- ☐ QI will implement all risk mitigation, corrective action, and client notification plans
- ☐ Update MCBH Potential HIPAA Breach Investigation and Assessment Information with action taken as part of implementation of risk mitigation, corrective action, and client notification plans

VI. Send any additional reporting requested by DHCS and complete mandated reporting of PHI breach to the United States Department of Health and Human Services (DHHS)

- ☐ Comply with any additional reporting requested by DHCS by sending an updated PIR to DHCS contract monitor, privacy officer, and information security officer
- ☐ Complete the US DHHS online reporting system at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html
- ☐ Update MCBH Potential HIPAA Breach Investigation and Assessment Information with all actions taken to comply with DHCS and DHHS reporting
- ☐ Send by interoffice mail completed US DHHS report, CA DHCS PIR,and MCBH Potential HIPAA Breach Investigation and Assessment Information to Health Department Privacy Officer at Health Department Administration (1270 Natividad)

405 Monterey County Health Department

Special and/or Unusual Incident Form

Reporting Agency/Program and telephone number	Name of Employee(s) Involved	Address/Location of Incident	Date of Incident	Date of Report

Brief Description of Incident (time, place, circumstances)	
Brief Description of Injuries, Property Damage, Fatalities	
Brief Description of other(s) involved	
Names or Description of witness(es)	
List of responding agencies	
Publicity of Incident	
Action(s) taken to maintain safety and security of work site	
Action(s) Planned	
Attachments	

Report Submitted by (print and Sign):	Date:
Supervisor (Signature)	Date:
Division Chief (Signature)	Date:

County use only:

HD Admin only: A copy of this report will be sent to and verbal notification was made to:

County Counsel	Date/Time:	Name of Contact:
CAO/HR	Date/Time:	Name of Contact:
Department Head	Date/Time:	Name of Contact:
Beta Healthcare Group	Date/Time:	Name of Contact
Director of Health (Signature)		Date:

CONFIDENTIAL Attorney/Client Privilege (When Completed)

Monterey County Health Department
Special and/or Unusual Incident Form
For Community Providers

Reporting Agency/Program and telephone number	Name of Employee(s) Involved	Address/Location of Incident	Date of Incident	Date of Report

Brief Description of Incident (time, place, circumstances)	
Brief Description of Injuries, Property Damage, Fatalities	
Brief Description of other(s) involved	
Names or Description of witness(es)	
List of responding agencies	
Publicity of Incident	
Action(s) taken to maintain safety and security of work site	
Action(s) Planned	
Attachments	

Report Submitted by (print and Sign):	Date:
Supervisor (Signature)	Date:
Division Chief (Signature)	Date:

County use only:

HD Admin only: A copy of this report will be sent to and verbal notification was made to:

County Counsel	Date/Time:	Name of Contact:
CAO/HR	Date/Time:	Name of Contact:
Department Head	Date/Time:	Name of Contact:
Beta Healthcare Group	Date/Time:	Name of Contact
Director of Health (Signature)		Date:

Fax

Date_____

From:

Program:

Phone:

Fax:

To:

- ☐ Mental Health Director's Office (831) 755-4980
- ☐ Quality Improvement Manager's Office (831) 831-755-4350

Regarding: Special Incident Report

Comments:

Was the Critical Incident Stress Management(CISM Team) Contacted for a debriefing? ☐ Yes ☐ No