



Monterey County Behavioral Health Policy and Procedure

Policy Number	322
Policy Title	Protected Health Information (PHI) Breach Notification and Mandatory Reporting
References	<ul style="list-style-type: none">• 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.

- 28
- 29
- 30
- 31
- 32
- 33
- 34
- 35
- 36
- 37
- 38
- 39
- 40
- 41
- 42
- 43
- 44
- 45
- 46
- 47
- 48
- 49
- 50
- 51
- 52
- 53
- 54
- 55
- 56
- 57
- 58
- 59
- 60
- 61
- 62
- 63
- 64
- 65
- 66
- 67
- 68
- 69
- 70
- 71
- 72
- 73
- “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.

- 74
- 75 3. A disclosure of PHI where a CE or BA has a good faith belief that
- 76 an unauthorized person to whom the disclosure was made would
- 77 not reasonably have been able to retain such information, for
- 78 example, sending PHI in the mail to the wrong address where the
- 79 mail is returned unopened to the post office as undeliverable, or
- 80 where a nurse mistakenly hands discharge papers to the wrong
- 81 patient, quickly realizes the mistake, and recovers the PHI before
- 82 the patient has time to read it.
- 83

84 **When there is suspicion of a "breach"**

85

86 Any employee, volunteer, student, agent, contractor, business associate or other

87 person or entity working on behalf of this facility who suspects that there may

88 have been an acquisition, access, use, or disclosure of "unsecured" PHI in a

89 manner not permitted by the Privacy Rule shall immediately notify their

90 supervisor and the MCBH Quality Improvement (QI) Team. The QI Team can be

91 contacted at (831) 755-4545. The QI Team will then immediately notify the

92 Monterey County Health Department (Health Department) Privacy Officer and

93 consult with Monterey County Counsel (County Counsel) regarding the situation.

94

95 **Assessment of the "breach"**

96

97 An assessment will be done in the case of every potential reportable breach to

98 determine whether it meets one of the three exceptions listed in the definitions

99 section of this policy or that based upon a risk assessment, it is determined that

100 there is a low probability that the PHI has been compromised. If the decision is

101 made to notify the patient and report the breach regardless of the outcome of the

102 assessment, an assessment need not be made. The decision to notify the

103 patient and report the breach must be done in consultation with the MCBH QI

104 Team, Health Department Privacy Office, and County Counsel.

105

106 If it is determined that it meets an exception, or that there is a low probability that

107 the PHI has been compromised based upon at least the four factors that must be

108 considered in the assessment as described above, the person making that

109 determination shall prepare written documentation of that determination and

110 submit it to the MCBH QI Team, who will retain it for at least six (6) years. The

111 MCBH QI Team will then send the written documentation to the Health

112 Department Privacy Officer and to County Counsel for review. Patient

113 notification and reporting to the DHHS is not required in the case of an exception

114 or determination that there is a low probability that the PHI has been

115 compromised.

116

117 **Breach Risk Assessment**

118 ***Note:*** A HIPAA breach risk assessment tool is available through MCBH QI to

119 assist in completing the necessary breach risk assessment. Contact MCBH QI at

120 831-755-4545 for additional information regarding the breach risk assessment
121 tool.

122
123 All risk assessment will be conducted by QI Team clinical staff, the Health
124 Department Privacy Officer, and/or County Counsel. When doing the risk
125 assessment as to whether the PHI has actually been compromised, staff
126 conducting the assessment shall address the following issues:

- 127
128 1. Nature and extent of PHI involved, including types of identifiers and
129 likelihood of re-identification (for example, if only a patient's first initial and
130 last name was released, with no other information on a list vs. a patient's
131 name, date of birth, and social security number, or a patient's HIV, mental
132 health or substance abuse treatment information)
- 133
134 2. The unauthorized person who used the PHI or to whom the disclosure
135 was made (for example, if the recipient also must comply with federal
136 privacy laws because it is a federal agency or is itself a CE)
- 137
138 3. Whether the PHI was actually acquired or viewed (for example, if IT
139 specialists assure through their investigation that patient data on a stolen
140 laptop was never accessed)
- 141
142 4. The extent to which the risk to the PHI has been mitigated (for example,
143 For example, did the recipient provide satisfactory assurances that the
144 PHI will not be further disclosed, was not read, and has been destroyed?)

145
146 Notification and reporting is not required if it is determined that there is a low
147 probability that the PHI has been compromised. However, the risk assessment
148 and written documentation determination must be retained for at least six (6)
149 years.

150
151 If it is determined that there was a breach, the patient must be notified and the
152 breach must be reported to the DHHS.

153 **Breach Notification to Individual whose PHI was Breached**

154
155 When: Notification must be made w/o reasonable delay and no later than sixty
156 (60) days after discovery. A breach is deemed discovered when an employee,
157 officer, or other agent of the covered entity or business associate other than the
158 individual committing the breach, knew or should reasonably have known about
159 the breach.
160

161
162 Law Enforcement Exception: if law enforcement asks you to delay
163 notification/reporting because it would impede a criminal investigation or cause
164 damage to national security, then you should delay notification/reporting until the
165 investigation is completed. If the request is made orally, you should document

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

169
170 How: Notification should be by first class mail to the individual's last known
171 address, unless the individual has specified a preference for email or other
172 means. If the patient lacks capacity, notify the personal representative (e.g.,
173 parent of a minor). If the patient is deceased, notify the next of kin.

174
175 If notification is urgent because of possible imminent misuse of the unsecured
176 PHI, you should notify individuals by phone or other means as appropriate;
177 additionally, written notification is still required.

178
179 If fewer than ten patients cannot be reached by first class mail, then substituted
180 means of communication should be employed. This may involve phone calls,
181 website notification, or use of the media, whichever is most likely to reach the
182 individuals.

183
184 Breach involving 10 or more patients who cannot be reached: If there are ten or
185 more individuals for whom there is insufficient or out-of-date contact information,
186 then one of the following is required:

- 187
- 188 • a conspicuous posting on the covered entity's home page of their website,
189 OR
 - 190
 - 191 • notice in major print or broadcast media (including major media where
192 individuals likely reside)
 - 193

194 Either method requires a minimum posting of 90 days and a toll free number that
195 an individual can call to find out if his/her unsecured PHI was included in the
196 breach.

197
198 Content of notice to individuals: When notifying individuals by any method, the
199 following information should be included in the notice that is provided:

- 200
- 201 • Brief description of what happened
 - 202 • Date of the breach, if known
 - 203 • Date of discovery of the breach
 - 204 • Description of types of information involved such as full name, date of
205 birth, home address, account number, disability code, etc.
 - 206 • Steps that individual should take to protect him/herself from potential harm
207 resulting from the breach
 - 208 • Brief description of what the CE is doing to investigate the breach, mitigate
209 losses and protect against further breaches
 - 210 • Contact procedures for individuals who have questions, which must
211 include a toll-free number, email address, website or postal address.

212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257

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.

258 If BA is acting as an agent, then the time to notify the individual runs from the
259 time of the breach, not from the time the CE learns of it. If BA is an independent
260 contractor, then notification time is based on the time CE is first notified of the
261 breach

262
263 The BA contract may specify whose responsibility it will be to provide notifications
264 (individuals should not receive two notices because duplicate notices about the
265 same breach could be confusing).

266
267 Note: The CE or BA is not responsible for a breach by a third party to whom it
268 permissibly disclosed PHI unless the third party is an agent of the BA or CE.
269

270 **Attachment 1: Protected Health Information Breach Reporting Procedures**

271

272 Steps to be taken:

- 273 The MCBH staff or contract provider directly involved in the incident and/or their
274 supervisor/manager will call MCBH QI at 831-755-4545 and provide a verbal report of the
275 suspected PHI breach to a member of the MCBH QI clinical team
- 276 **NOTE: *The verbal report to MCBH QI must be done in the same day as the***
277 ***discovery of the potential breach!***
- 278 For the verbal report to QI, be ready with specific information regarding the
279 suspected PHI breach, including a list of clients possibly affected
 - 280 If after hours, leave a message on the confidential MCBH QI voicemail regarding
281 the suspected breach and a clinical staff member will contact you the following
282 business day. Leave the following information in the voicemail:
 - 283 Name
 - 284 Team, program, or agency name
 - 285 Contact number
 - 286 Supervisor or program manager name
 - 287 Supervisor or program manager contact number
- 288 Complete the Monterey County Health Department Unusual or Special Incident Report
289 per MCBH Policy 123 – Unusual Incident Reporting
- 290 Unusual or Special Incident Report needs to include, at minimum, detailed
291 information regarding the following:
 - 292 Circumstances of the suspected breach
 - 293 Location (including full address) of suspected breach
 - 294 A list of client IDs whose PHI is involved in the suspected I breach
 - 295 A detailed description of the PHI possibly impacted by the suspected
296 breach. The information should contain but not be limited to the
297 following:

298 **NOTE: *This is extremely critical information as the type of PHI affected***
299 ***determines the level of mitigation and correction MCBH needs to engage***
300 ***in***

 - 301 What type of media was the PHI contained in (e.g., electronic, paper)?
 - 302 What type of PHI was potentially breached (e.g., client IDs, names,
303 social security numbers)?
 - 304 How was the PHI stored (e.g., Was the PHI a list of client IDs or client
305 names? Was this list placed with a calendar with client names and
306 appointments? Was the staff's MCBH business card attached or near?)
 - 307 Fax completed report to the following:
 - 308 MCBH QI – Fax: 831-755-4350
 - 309 MCBH Administration – Fax: 831-755-4980
- 310 Please have reporting staff and supervisor(s)/manager(s) prepared for follow up
311 questions and inquiries from MCBH QI.
- 312

313 **Attachment 2: QI Breach Assessment and Reporting Procedures**
314

315 **NOTE:** The following procedures are for the ***Quality Improvement Team ONLY***
316

- 317 I. Inform County Counsel and Health Department Privacy Officer via email of potential PHI
318 breach
319 QI clinical staff will complete California Department of Health Care Services (DHCS)
320 Privacy Incident Reporting Form (“PIR”) located at
321 <http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/CountiesOnly.aspx> with as
322 much information as possible
323 QI will send PIR to County Counsel and Health Department Privacy Officer for review
324 with clear indication that reply is needed ASAP in order to comply with DHCS
325 timelines (*within 72 calendar hours*)
326 County Counsel staff to be notified:
327
 - Stacy Saetta
 - Anne Brererton
328 Health Department Privacy Officer to be notified:
329
 - Molly Hubbard
330 Cc: Amie Miller, MCBH QI Services Manager
331
332
333
- 334 II. Notify the California Department of Health Care Services (“DHCS”) of potential PHI
335 breach as soon as County Counsel and Health Department Privacy Officer replies
336 regarding initial PIR
337 Once County Counsel and Health Department Privacy Officer replies, QI will forward
338 PIR via email to DHCS contract monitor, privacy officer, and information security
339 officer
340 DHCS contacts to be informed:
341
 - Contract monitor: Erika.Cristo@ca.dhcs.gov (*NOTE: check on a*
 - 342 *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
343 Cc: MCBH QI Services Manager
344 Cc: Health Department Privacy Officer
345
346
347
348

- 350 III. Conduct PHI breach assessment and develop strategies to mitigate harm
- 351 QI clinical staff will gather additional information regarding the incident and compile
- 352 gathered information in MCBH Potential HIPAA Breach Investigation and
- 353 Assessment Information form
- 354 QI clinical staff will utilize the California Hospital Association (6/13) HIPAA Breach
- 355 Decision Tool and Risk Assessment Documentation Form to determine if the
- 356 reported incident was an actual PHI breach and assess the risk level of the breach
- 357 If the HIPAA Breach Decision Tool and Risk Assessment Documentation Form
- 358 indicates that a breach occurred, QI staff will develop risk mitigation plan, corrective
- 359 action plan, and client notification plan (in compliance with standards provided by
- 360 DHCS)
- 361 QI clinical staff will update DHCS PIR form with relevant information from the MCBH
- 362 Potential HIPAA Breach Investigation and Assessment Information and the HIPAA
- 363 Breach Decision Tool and Risk Assessment Documentation forms
- 364 List of affected client IDs does not need to be transferred to DHCS PIR
- 365 Privileged communications between County Counsel and QI should not be
- 366 entered into DHCS PIR
- 367 QI clinical staff will submit the updated DHCS PIR form along with notification plan
- 368 (including general versions of beneficiary notification letters) for review to:
- 369 County Counsel
- 370 Risk management consultant (if available), and
- 371 Health Department Privacy Officer
- 372 Cc: MCBH QI Services Manager
- 373
- 374
- 375 IV. Submit an updated PIR to DHCS within the specified time line (*10 working days*)
- 376 Make changes to DHCS PIR requested by County Counsel, risk management
- 377 consultant (if available), and Health Department Privacy Officer
- 378 Once changes are made to DHCS PIR, QI will forward PIR via email DHCS contract
- 379 monitor, DHCS Privacy Officer, and DHCS Information Security Officer
- 380 Cc: MCBH QI Services Manager
- 381 Cc: Health Department Privacy Officer
- 382
- 383
- 384 V. Follow through on risk mitigation, correction action, and client notification plans
- 385 QI will implement all risk mitigation, corrective action, and client notification plans
- 386 Update MCBH Potential HIPAA Breach Investigation and Assessment Information
- 387 with action taken as part of implementation of risk mitigation, corrective action, and
- 388 client notification plans
- 389

390
391
392
393
394
395
396
397
398
399
400
401
402

403
404

- 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/brinstructio.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)

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/Time:	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/Time:	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