SAN MATEO COUNTY HEALTH
BEHAVIORAL HEALTH & RECOVERY SERVICES

DATE: December 6, 1993

BHRS POLICY: 93-11

SUBJECT: Critical Incident Reporting, Including Breaches and Security Incidents, for Mental Health and AOD Providers

AUTHORITY: 45 CFR Part 160 (HIPAA Privacy Regulations); California State Evidence Code, Section 1157; W&I Code, 9 (1810.440), Divisional, the Health Information Technology for Economic and Clinical Health Act (HITECH), Health Insurance Portability and Accountability Act HIPAA, ODS (Organized Delivery System) Waiver Contract with DHCS Exhibit G, DHCS Managed Care Contract with San Mateo County, Divisional

AMENDED: January 24, 2002, November 15, 2002, November 14, 2012, December 8, 2016, June 7, 2017, August 31, 2017, November 18, 2019 (technical edit)

ATTACHMENTS: A. Critical Incident Report Form – Amended December 8, 2016, June 7, 2017
B. Breach Reporting Decision Tree – Added December 8, 2016

BACKGROUND:
The Critical Incident Report is a CONFIDENTIAL reporting tool to document occurrences inconsistent with usual administrative or medical practices. A Critical Incident is an event or situation that creates a significant risk of substantial or serious harm to the physical or mental health, safety or well-being of a client, family member, volunteer, visitor or staff. Reporting and analyzing Critical Incidents is a recognized Quality Improvement (QI) mandate and process.

The Critical Incident reporting system also provides a mechanism to organize information relating to potential breaches of client privacy, and to document mitigation efforts once a breach is recognized. This does not replace other reporting requirements, such as Community Care Licensing (CCL), Alcohol and other Drug (AOD)/Substance Use Disorders (SUD) reporting, child/elder abuse reporting, and any other mandated reporting; all providers will continue to meet their particular licensing requirements.

NOTE:
This policy relates to the *communication and reporting* of a Critical Incident. It does not address the immediate clinical or administrative *management* of that incident.

PURPOSE:
The specific purposes of Critical Incident Reporting within Behavioral Health and Recovery Services (BHRS) are:

- To provide immediate notification to BHRS administration of unusual events within our system for the purpose of timely investigation and response.
- To gather information to identify patterns, solve practical problems and develop or update policies and procedures.
- To provide a risk management/QI tool that will facilitate procedure development, in-service education, facility modifications, etc., in order to improve services and reduce the likelihood of future Critical Incidents.
- To provide a protected means of data collection that can be reviewed by BHRS Administration, Quality Management (QM), risk management and legal staff in potential liability questions.
- To provide a means for auditing and assessing potential breaches of confidentiality/privacy required by Federal Privacy Regulations and State laws and to assess compliance with the Privacy Rule.
- To ensure that mandated reporting occurs as required.

POLICY:
All San Mateo County BHRS staff, on-site contractors, contracted agencies and their staff members, students and volunteers are required to document and report critical incidents to BHRS administration in a timely manner using the attached form. On approval of QM, agencies may report using alternative forms. Trainings on Critical Incidents and Confidentiality/HIPAA are available at QM's website: http://www.smchealth.org/bhrs/providers/ontrain

DEFINITIONS:

- A Critical Incident (in some settings, called a sentinel event or unusual occurrence) is defined as any circumstance or event that deviates from usual procedure or practice within BHRS and has the real or potential negative effect on the health and/or safety of clients, family members or staff; client rights to confidentiality/privacy of health information, or the relationship of BHRS to the community. The categories of incidents on the Critical Incident Report form (Attachment A) indicate areas that require reporting but do not limit the range and scope of reportable incidents.

- A Breach is the acquisition, access, modification, destruction, use or disclosure of protected health information (PHI) by BHRS staff or a contractor in a manner not permitted by Federal and State laws and regulatory requirements.

- A Security Incident is the attempted or successful unauthorized access, use, disclosure, modification or destruction of PHI, systems operations or confidential data by BHRS staff or a contractor who is providing services on behalf of BHRS.

PROCEDURE:

FOR BHRS COUNTY TEAMS/PROGRAMS:

The Critical Incident Report form will be completed immediately after the event, if possible, after the incident for emergency or very urgent incidents and no later than 24 hours. For non-emergency incidents, they must be reported by the next business day at the latest.

QM may also be notified by telephone to expedite immediate notification. A completed Critical Incident Report form is still required following a telephone notification within the timeline specified above. The report must be emailed or faxed to BHRS QM. This information can be found at the top of the Critical Incident reporting form. QM will forward the report to the Deputy Directors of Adult/Older Adult and Child/Youth Services, the BHRS Assistant Director, Medical Director and Director within the same day of receiving the Critical Incident Report Form.

If a significant breach or security incident happens after hours, on a weekend or holiday that poses harm to clients or data, utilize your program's on-call management system to inform management immediately. Management will contact the BHRS Compliance Officer or Director who will either report the incident to the DHCS Information Protection Unit (See #3 on page 4 for DHCS reporting procedure) or designate the reporting to another BHRS manager.

The person most closely involved or most knowledgeable about the circumstances should write the report. Reports may be written and submitted by any other knowledgeable staff if necessary. The person completing the report submits the report to their supervisor, unit chief, or medical chief, who then reviews, signs, and submits the report to QM within the timelines specified above. If the supervisor, unit chief, and medical chief are not available, the report is submitted by the reporting staff directly to QM within the timelines specified above. It is not acceptable to collect and submit the reports in batches.

Critical Incident Reports must never be filed or referenced in a client's chart or in an employee's personnel record. *However, the circumstances of the event and the services provided shall be appropriately documented in the client record.* In circumstances where the event has necessitated other reports, for example to a legal authority or to Workers' Compensation, a Critical Incident Report is still required.

FOR CONTRACTORS:

The Critical Incident Report shall be completed and faxed to QM the same day the incident occurred or within 24 hours at the latest. BHRS QM and your contract manager may also need to be notified by telephone; this does not remove the requirement for immediate written alert.

Critical Incident Reports must never be filed or referenced in a client's chart. *However, the circumstances of the event and the services provided shall be appropriately documented in the client record.*

It is not acceptable to collect and submit the reports in batches. No hard copies or electronic copies of the Incident Report are to be kept by the person reporting the incident. Internal

copies may ONLY be maintained by the contractor's compliance officer/quality management as part of quality oversight. These must be stored in a secure location without general access. All other copies must then be shredded or deleted.

FOR ALL POTENTIAL BREACHES OF CONFIDENTIALITY:

Breaches and security incidents involving the unauthorized access, use, modification, disclosure, or destruction of protected health information (PHI) are types of Critical Incidents. Several state and federal laws govern how suspected breaches must be addressed within mandated timelines. It is each BHRS employee's and contractor's responsibility to know what a breach is and how to report it to QM. Suspected breaches should always be reported to QM. The QM Manager is the Privacy Officer of BHRS as designated by the San Mateo Medical Center (SMMC) Privacy Officer.

The following steps will be taken in case of a suspected breach or security incident:

1. The BHRS staff or contractor who made or became aware of the potential breach or security incident must notify QM that same day by completing the Critical Incident Report form (Attachment A) and by telephone. Staff should consult their supervisor or manager as needed.
    a. Notify QM immediately by telephone call and in addition, email/fax a completed Critical Incident form upon the discovery of a security incident or breach of unsecured PHI in electronic media or in any other media if the PHI was, has the potential to be, or is reasonably believed to have been, accessed or acquired by an unauthorized person.
    b. Notify QM within that same day (**within one hour if Social Security Administration data**) by email or fax of the discovery of any suspected security incident, intrusion or unauthorized access, use or disclosure of PHI in violation of HIPAA, California Privacy Law, the HITECH Act and 42 CFR part 2 or suspected/potential loss of confidential data. A breach shall be treated as discovered as of the first day that the breach is known or should have been known to any person exercising reasonable diligence. Here "any person" is identified as the person who committed the suspected breach, or any other person who is an employee, officer, contractor or other agent of BHRS.
    c. If a significant breach or security incident happens after hours, on a weekend or holiday that poses harm to clients or data, utilize your program's on-call management system to inform management immediately. Management will contact the BHRS Compliance Officer or Director who will either report the incident to the DHCS Information Protection Unit (See #3 below for DHCS reporting procedure) or designate the reporting to another BHRS manager.

2. **QM will investigate and report**. QM will immediately investigate any suspected or known security incident, breach, unauthorized access, use or disclosure of PHI. BHRS QM/Privacy Officer will evaluate all suspected breaches or security incidents using the Breach Reporting Decision Tree (Attachment B). QM will consult with the San Mateo County Security Officer, and BHRS Compliance Officer as needed. If a breach or security incident occurred, QM will report the breach to the proper authorities.

3. **For all breaches, QM will submit a DHCS "Privacy Incident Report"** *w*ithin 72 hours of the discovery, **and 24 hours for Substance Use Disorders programs and breach of Social Security Administration information,** to the DHCS Information Protection Unit (IPU) at the Office of HIPAA Compliance (OHC). The initial "Privacy Incident Report" will contain all required information to the extent known at that time. QM will follow further instructions received from the IPU. QM will notify DHCS by calling the Information Protection Unit (916-445-4646, 866-866-0602) and emailing notification to: privacyofficer@dhcs.ca.gov Updated forms will be submitted to the DHCS as more information becomes available.

   The current version of the form is available at the DHCS OHC website: www.dhcs.ca.gov, then select "Privacy & HIPAA" and then "Business Partner" or at: http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/DHCSBusinessAssociatesOnly.aspx

4. **QM will submit a final report including a corrective action plan**. A complete report of the investigation will be provided to the DHCS Program Contract Manager and the IPU within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. After the investigation is completed, an updated "Privacy Incident Report" form, including an assessment of all known factors relevant to a determination of whether a breach occurred under applicable provisions of HIPAA and the HITECH Act and any other regulations applicable must be submitted. The report shall also include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. If the DHCS requests information in addition to that listed on the "Privacy Incident Report" form, QM shall make reasonable efforts to provide DHCS with such information.

REVIEW, INVESTIGATION, ANALYSIS, AND COUNTERMEASURES FOR ALL INCIDENTS:

A managerial review is required for *all incidents*. This review will include a root cause analysis and the identification of countermeasures to prevent future such occurrences. QM will initiate the review with support and participation from one or more of the following BHRS Executive staff: Deputy Directors, the Medical Director, the Assistant Director, and the Director. These staff will support the work of the unit management team to ensure understanding of the incident and identification of preventative measures to minimize the likelihood that the incident is repeated and to ensure that lessons are learned that benefit BHRS, the Health System, and the County.

The QM Manager, Medical Director and/or other BHRS leadership may investigate, monitor needed improvements or otherwise address issues identified in the Critical Incident Report.

The report will be reviewed for QI/risk management issues and maintained securely at the QM office with other protected material. No copies of the original report are to be made or retained by other BHRS staff and a copy can only be kept by the quality/risk manager of contracted agencies as outlined in the Contractor section above.

The QM Manager will present summary data annually or as needed, to the Quality

Improvement Committee for monitoring and oversight functions.

Approved: *Signature on File*
Scott Gilman, MSA
BHRS Director