County of San Bernardino  
Department of Behavioral Health  

Privacy or Security Incident Policy  

Effective Date  
07/01/2010  

Approval Date  
09/15/2014  

CaSonya Thomas, Director  

Policy  
It is the policy of the Department of Behavioral Health (DBH) to adhere to state and federal regulations pertaining to the reporting of privacy and/or security incidents, including breaches.  

Purpose  
To provide the DBH workforce with guidance on the requirements for identifying a privacy or security incident, individual responsibility for reporting an incident, and how to report an incident to the DBH Office of Compliance immediately upon discovery.  

Definitions  

Assist in the Administration of the Medi-Cal Program: Performing an administrative function on behalf of Medi-Cal, such as verifying Medi-Cal eligibility of a client.  

Privacy/Security Incident: The attempted or successful unauthorized access, use, disclosure, modification, or destruction of PHI or interference with system operations in an information system that does not result in a breach.  

Medi-Cal PII: Information directly obtained from Medi-Cal Eligibility Data System (MEDS) in the course of performing an administrative function on behalf of Medi-Cal that can be used alone, or in conjunction with other information to identify a specific individual.  

Personally Identifiable Information (PII): Any information maintained by DBH electronically or paper format which can potentially be used to uniquely identify, contact or locate County employees or members of the public.  

Protected Health Information (PHI): Individually identifiable health information relating to the past, present or future physical or mental health or condition of a client; the provision of health care to a client; or the past, present or future payment for the provision of health care to a client transmitted or maintained in any form or medium (electronic, paper, microfiche or verbal).  

Unauthorized Access: Inappropriate/impermissible entry, contact, review, opening or viewing of employee, public or client information without direct need for medical diagnosis, treatment, business purpose or other lawful use; and any other unlawful use not permitted by state or federal laws governing the use or disclosure of confidential information, medical or otherwise personal.  

Unauthorized Disclosure: Inappropriate/impermissible release, announcement, publication or statement of employee, public or client PHI without direct need for medical diagnosis, treatment, business purpose or other lawful use; and any other unlawful release not permitted by state or federal laws governing the use or disclosure of confidential information, medical or otherwise personal.  

Continued on next page
Unauthorized Use: Inappropriate/impermissible handling, application, operation or management of employee, public or client information without direct need for medical diagnosis, treatment, business purpose or other lawful use; and any other unlawful application not permitted by state or federal laws governing the use or disclosure of confidential information, medical or otherwise personal.

DBH Workforce: County employees, paid and unpaid interns, volunteers, contractors and contract agencies that provide clinical or administrative services for the DBH.

The following are examples of actions that may be privacy or security incidents. Staff is required to report to the DBH Office of Compliance immediately upon discovery. Examples include, but are not limited to the following:

- Faxing or emailing PHI/PII to the wrong recipient
- Emailing PHI/PII to anyone outside the County network, including yourself, without encryption (password protection is not encryption)
- Sending correspondence to the incorrect client
- Releasing PHI/PII to a person or entity with an expired Authorization for Release of Protected Health Information
- Misplacing/losing a medical record after a thorough search
- Accessing/using DBH and/or County resources to verify if family, friends or acquaintances are DBH clients
- Accessing, using or disclosing information obtained from MEDS other than to assist in the administration of the Medi-Cal Program
- Accessing, or peeking into, a medical record you did not need to access for a legitimate business purpose or to perform your job
- Being the victim of theft where DBH medical records or DBH property are taken
- Leaving medical records or PHI/PII in an unattended vehicle
- “Checking in” baggage containing medical records or PHI/PII on modes of public transportation; not keeping it/them in personal custody as carry on
- Giving yours or using another’s password/log in
- Leaving medical records or PHI/PII unsecured, i.e.; open and unattended on the desk, unlocked medical charts, unlocked PII, etc.
- Allowing unauthorized persons in the work area without a legitimate business purpose
- Discussing with or disclosing to others PHI/PII without a legitimate business purpose and/or without authorization from the client
- Discarding PHI/PII or medical records improperly and/or not in accordance with retention timeframes

Continued on next page
Identification of a Privacy or Security Incident (continued)

**Important Note:** The above examples may include inadvertent errors, negligence or even malicious intent. However, no matter the degree of access, use or disclosure, the DBH Office of Compliance must investigate the incident to determine if it is a breach reportable to State/Federal agencies.

Responsibilities and Reporting an Incident or Breach

There are various state agreements and state/federal regulations guiding the DBH Office of Compliance as to breach reporting requirements, including time frames. Due to the varied requirements, the following table illustrates the responsibility of the applicable DBH Workforce:

<table>
<thead>
<tr>
<th>Responsible Party</th>
<th>Responsibility</th>
</tr>
</thead>
</table>
| DBH Workforce               | • Report any privacy/security incident immediately, but not later than the date discovered:  
                                 |  DBH Office of Compliance  
                                 |  Office (909) 388-0879  
                                 |  Hotline (800) 398-9736  
                                 |  • Email Compliance_Questions@dbh.sbcounty.gov  
                                 | • Adhere to the DBH contract regarding reported breaches within its agency:  
                                 |  o Reporting to DBH within the required timeframe  
                                 |  o Investigating the reported breach  
                                 |  o Reporting the findings to DBH  
| DBH Contract Agencies       | • Notify applicable state agency(ies), as required  
                                 | • Investigate facts of the privacy/security incident, which may include but are not limited to the following:  
                                 |  o Conducting interviews with employee(s) and/or individuals involved, as necessary  
                                 |  o Gathering documentation, data, etc.  
                                 |  o Verifying what information was at risk of compromise  
                                 | • Determine if a reportable breach has or has not occurred  
                                 | • Notify the client(s) affected by the breach, as required by regulation  
                                 | • Prepare formal breach report for applicable agency(ies)  
                                 | • Issue memo to applicable deputy director and program manager including recommended corrective action, if applicable  
                                 | • Provide guidance to applicable program, as needed  
                                 | • Follow-up with program to ensure corrective actions are completed and/or addressed  
| DBH Office of Compliance    | • Complete corrective action, if applicable  
| DBH Program                 |                                                                                                                                               |

*Continued on next page*
Violations

Members of the DBH Workforce may be subject to the following actions due to a privacy/security violation:

- Corrective action including but not limited to receiving re-training on privacy and security measures, reviewing existing policy and signing policy acknowledgement forms
- Loss of MEDS access
- Disciplinary action, up to and including termination of employment
- Civil or criminal liability

Note: The action taken in response to a privacy or security incident or breach will be based on the violation levels as indicated in the Privacy and Security Violation Sanctions Policy.

Failure to Report

The omission or failure to report a privacy or security incident may subject members of the DBH Workforce to disciplinary action, up to and including termination.

References

California Civil Code, Section 56 et al., California Confidentiality of Medical Information Act
Medi-Cal Privacy and Security Agreement
Social Security Act, Sections 1137 and 453
Title 45 of the Code of Federal Regulations, Section 164 et al., Health Insurance Accountability and Portability Act of 1996
Welfare and Institutions Code, Section 14100.2

Related Policies and Procedures

County of San Bernardino Policy Manual:
- 14-02, Non-Public Personally Identifiable Information
- 14-03, Protection of Individually Identifiable Health Information

County of San Bernardino Standard Practice:
- 14-03SP1, Protection of Individually Identifiable Health Information

DBH Standard Practice Manual:
- COM0943-1, MEDS Access and Contacts Procedure
- IT5009, User I.D. and Password Policy
- COM0901, Sending Confidential Information by Facsimile Policy
- IT0909, Electronic Transfer of Client Protected Health Information – Internet and Intranet Policy
- IT5008, Device and Media Controls Policy
- COM0907, Unauthorized Access of Confidential Medical Records Policy
- COM0924, Workstation and System Security Policy
- COM0925, Data Integrity Policy

Continued on next page
Related Policies and Procedures (continued)

DBH Standard Practice Manual:
- COM0926, Privacy and Security Violation Sanctions Policy
- IT5004, Computer and Network Appropriate Use Policy
- IT5005, Electronic Mail Policy
- IT5006, Remote Access Policy
- COM0905, Client Privacy and Confidentiality of Protected Health Information