

Department of Behavioral Health ANNOUNCEMENT



Compliance



Behavioral Health

Compliance Corner

Stay in-the-know, by reading below.

Newly Posted Departmental Policies, Procedures, and Forms

The following are newly posted departmental policies, procedures, notices, and forms from February through March.

Please review, as each DBH staff member is responsible for familiarization with department notices, policies, procedures, and forms. These items can be found on the DBH Website, under the "For Agencies" drop down menu in the section titled "Documents." You can locate each document by clicking the appropriate tab and typing the title or number into the search box on the right. You can also search by sorting the column titled "Name" (by clicking on it) and locating the document alphabetically.

Revised Policies and Procedures:

- BOP3030 Prepaid Cards Policy

- BOP3030-1 Prepaid Cards Procedure
- CLP0819 Duty to Protect Policy
- CLP0819-1 Duty to Protect Procedure

New Forms:

- CLP063 Duty to Protect Intended Victim Letter
- CLP070 Specialty Crisis Note

Revised Forms:

- COM004_E Notice of Privacy Practices and Acknowledgement of Receipt of Notice of Privacy Practices
- COM004_M Notice of Privacy Practices and Acknowledgement of Receipt of Notice of Privacy Practices (Mandarin)
- COM004_S Notice of Privacy Practices and Acknowledgement of Receipt of Notice of Privacy Practices (Spanish)
- COM004_V Notice of Privacy Practices and Acknowledgement of Receipt of Notice of Privacy Practices (Vietnamese)

For more information, contact Policy Management Unit by email or phone at DBHPMUquestions@dbh.sbcounty.gov or (909) 388-0879.

Newly Posted Departmental Policies, Procedures, and Forms

Need a myAvatar Staff/Billing Number?

To record and bill for services in myAvatar, all direct service providers are required to complete a Staff Master Worksheet. Prior to completing the Staff Master Worksheet, the provider must obtain a National Provider Identifier (NPI) number, which can be requested through the National Plan & Provider Enumeration System (NPPES).

Click the link below to view the updated Staff Master Guidance

Staff Master Guidance Flyer

Updated Privacy & Security Incident Reporting Form – What You Need to Know

The Privacy & Security Incident Reporting Form (**COM042**) has been refreshed to include new reporting fields. These updates help ensure that all the vital information needed to mitigate incidents is captured.

Detailed Description of Privacy Incident:

Clinic/Program Involved:
 DBH: Program
 Contractor Agency

Date Discovered: _____ # of Clients Affected: _____
Date Occurred: _____ # of Minors: _____
Date Reported: _____ [DBH Only] Client ID#: _____

myAvatar [Misfiling Only] Correct Client ID # _____ Incorrect Client ID# _____
myAvatar [Misfiling Only] Correct Client ID # _____ Incorrect Client ID# _____

Was Mental Health PHI Involved? Yes (WIC 5328/HIPAA regs applicable) No

Was SUD PHI Involved? Yes (42 CFR Part 2 regs applicable) No

Note: Protections under 42 CFR Part 2 apply only when a client's SUD PHI originates from a federally assisted Part 2 program. If it does not, the information is not protected under Part 2.

Was the PHI or PII in question acquired or used in the administration of the Medi-Cal program? Yes (Medi-Cal Data Privacy and Security Agreement with DBH/DHCS Applies) No

Responsible Party who caused incident (Name, title, email address, and telephone number and job duties): _____

Which of the 18 HIPAA identifiers of PHI were potentially compromised (select all that apply):

<input type="checkbox"/> Client Name	<input type="checkbox"/> Social Security Numbers	<input type="checkbox"/> Device attributes or serial numbers
<input type="checkbox"/> Street address, city, county, or zip code	<input type="checkbox"/> Medical record numbers (Avatar/Simon, etc...)	<input type="checkbox"/> Digital identifiers, such as website URLs
<input type="checkbox"/> DOB <input type="checkbox"/> Date of Admission	<input type="checkbox"/> Health insurance beneficiary numbers	<input type="checkbox"/> Biometric elements, including finger, retinal, and voiceprints
<input type="checkbox"/> DOD <input type="checkbox"/> Date of Discharge		
<input type="checkbox"/> Other Date:		
<input type="checkbox"/> Telephone numbers	<input type="checkbox"/> Account Numbers	<input type="checkbox"/> IP Addresses
<input type="checkbox"/> Fax Numbers	<input type="checkbox"/> Certificate/License Numbers	<input type="checkbox"/> Full face photographic images
<input type="checkbox"/> Email Addresses	<input type="checkbox"/> Vehicle Identifiers	<input type="checkbox"/> Other identifying numbers or codes



Behavioral Health

303 E. Vanderbilt Way San Bernardino | (909) 388-0900

www.SBCounty.gov

Privacy and Security Incident Reporting Form

<p>Mitigation Efforts</p>	<p>Information is: <input type="checkbox"/> Electronic <input type="checkbox"/> Hard Copy <input type="checkbox"/> Verbal</p> <input type="checkbox"/> Written attestation was secured (please provide) <input type="checkbox"/> PHI was secured, recovered, deleted from both email inbox and deleted items folder (if ePHI). <p>Were any other agencies notified?</p> <p>Was a police report filed (include #)?</p> <p>← Enter on the left:</p> <p>What mitigating efforts were taken thus far? Describe what action was taken to ensure the incident was immediately addressed and further threats of PHI/PII exposure was mitigated.</p> <p>For additional reporting and privacy incident guidance, see the Privacy Incident Policy (COM0944).</p>
	<p>Administrative & Personnel Information</p> <p>Direct supervisor's name, title, and credential(s) for the party that caused the incident:</p> <p>Supervisor was notified on (MM/DD/20XX):</p> <p>Has this party been involved in a potential privacy incident before? (Is this incident their second, third, fourth, etc.?) If yes, was it for the same type of incident (if known)?</p> <p>Date of last HIPAA annual training for party that caused the Incident (supervisor to provide - MM/DD/20XX):</p> <p>Deputy Director over program:</p> <p>Send all PHI in this form, copies of emails, forms, etc. that were compromised encrypted.</p>
<p>SUBMIT THIS FORM TO: DBH-PrivacyIncidents@dbh.sbcounty.gov</p>	

Remember: You Play a Key Role in Keeping PHI Safe

All DBH staff and contract providers should report, respond, and act quickly if a privacy or security incident occurs. Your prompt action helps protect our clients and keeps everyone compliant.

What should you do if an incident occurs?

- Notify your supervisor and the DBH Office of Compliance immediately.
- Submit the **COM042** form at the time of reporting to DBH-PrivacyIncidents@dbh.sbcounty.gov.
- Take immediate steps to mitigate any potential unauthorized access to PHI.
- For additional guidance, refer to the Privacy Incident Policy (**COM0944**).

Click below to view the updated Privacy & Security Incident Reporting Form.

[Privacy & Security Incident Reporting Form](#)

Coming Soon: Updated Authorization Form

DBH will release a revised Authorization for Use and Disclosure of PHI form to align with DHCS requirements, effective July 1, 2026. Please watch for additional guidance and be prepared to begin using the new form when it becomes available.

Department of Behavioral Health - WEBMASTER
(909) 386-9730

Our job is to create a county in which those who reside and invest can prosper and achieve well-being.

www.SBCounty.gov/DBH

County of San Bernardino Confidentiality Notice: This communication contains confidential information sent solely for the use of the intended recipient. If you are not the intended recipient of this communication, you are not authorized to use it in any manner, except to immediately destroy it and notify the sender.