

## County of San Bernardino Department of Behavioral Health

### HIPAA BASELINE PRIVACY & SECURITY WALKTHROUGH AUDIT

(Conducted quarterly with the safety inspection and submitted at the Safety Committee meeting. Maintain a copy in [Section 9](#) of the DBH Safety Binder)

| Location/Program/Dept.                                 | Phone  | Indicators: C = Compliant, P = Partial Compliance, N = Not Compliant, NA = Not Applicable |   |   |    | Comments/References/Violation(s) |
|--|--|---|---|---|----|----------------------------------|
| Manager/Supervisor/LSC                                 | Date   | C   | P | N | NA |                                  |
| <b>NOTICE OF PRIVACY PRACTICES</b>                     |  |   |   |   |    |                                  |
| 1  | Privacy notice posted/accessible to patients   |   |   |   |    |                                  |
| 2  | Physical Layout – Computers & Confidential Information Secure                                      |   |   |   |    |                                  |
| 3  | Acknowledgements obtained  |   |   |   |    |                                  |
| <b>PROPER DISPOSAL OF CONFIDENTIAL INFORMATION-PHI</b> |  |   |   |   |    |                                  |
| 4  | Confidential information is disposed of properly (not in trash, not in break rooms, etc.)          |   |   |   |    |                                  |
| 5  | Transportation of records is secure (interoffice mail sealed)                                      |   |   |   |    |                                  |
| 6  | Storage of patient records and confidential information is secure (records storage rooms locked)   |   |   |   |    |                                  |
| 7  | Recycle bins and trash receptacles contain no confidential information                             |   |   |   |    |                                  |
| 8  | Confidential shredding bins are not to full (e.g., confidential information cannot be seen)        |   |   |   |    |                                  |
| <b>PRIVACY/SECURITY IN WORKSTATION/WORK AREA</b>       |  |   |   |   |    |                                  |
| 9  | Area layout conducive to privacy (all confidential info secured, desks not cluttered, etc.)        |   |   |   |    |                                  |
| 10   | Computer monitors w/PHI not visible or viewable to unauthorized staff                              |   |   |   |    |                                  |
| 11   | Unattended PCs are locked/logged off   |   |   |   |    |                                  |
| 12   | Portable PC's, laptops, PDA's, removable media (e.g. CD's) securely stored                         |   |   |   |    |                                  |
| 13   | Electronic data storage devices properly disposed of   |   |   |   |    |                                  |
| 14   | Fax machines located in secured areas  |   |   |   |    |                                  |
| 15   | Fax machines have been cleared of any confidential information                                     |   |   |   |    |                                  |
| 16   | Evidence showing that cover letters are used when faxing PHI                                       |   |   |   |    |                                  |
| 17   | Printers/Copiers are secured (printouts not left on printer, copy machines used securely)          |   |   |   |    |                                  |
| 18   | Restricted areas and/or systems are secured from inappropriate access and theft                    |   |   |   |    |                                  |
| <b>EMPLOYEE AWARENESS</b>                              |  |   |   |   |    |                                  |
| 19   | Badge/ID is properly utilized (worn at all times; not turned around, not shared, clearly visible)  |   |   |   |    |                                  |
| 20   | Staff use their own user ID's and passwords  |   |   |   |    |                                  |
| 21   | Staff have read all policies and procedures (training logs/acknowledgement signed – HIPAA-related) |   |   |   |    |                                  |

## County of San Bernardino Department of Behavioral Health

|  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|
| 22   | Policies and procedures are up to date (both privacy and security in place)  |  |  |  |  |  |
| 23   | Staff shows awareness of privacy/security requirements evidenced in practice (e.g., no speaking of confidential information in public areas) |  |  |  |  |  |
| <b>EVALUATION PROCEDURES-RISK ASSESSMENT</b> |  |  |  |  |  |  |
| 24   | Periodic privacy/security reminders are posted or provided to staff via staff meetings   |  |  |  |  |  |
| 25   | Privacy & Security Official(s) designated and authority established, documented  |  |  |  |  |  |
| 26   | Periodic privacy & security risk assessment conducted  |  |  |  |  |  |
| 27   | Risk assessment deficiencies corrected   |  |  |  |  |  |

**Corrective Action Plans/Corrections due 30 days from receipt of assessment. Forward to the Disaster & Safety Coordinator.**

**Auditor Information**

Auditor Name: \_\_\_\_\_ Auditor Telephone Number: \_\_\_\_\_

Date sent to Department HIPAA Compliance Officer: \_\_\_\_\_

Comments:

**DEPT HIPAA COMPLIANCE OFFICE USE ONLY**

Date Audit Received: \_\_\_\_\_ Corrective Action Required  Yes  No Due Date: \_\_\_\_\_

Date Copy Provided to Manager: \_\_\_\_\_ Audit Copy Sent to Dept Head  Yes  No

Follow up: Corrective Action Plans/Corrections must be completed/received within 30 days from receipt of the assessment. Notify Association Admin if CAP/Corrections are delinquent.

CAP: Received \_\_\_\_\_  
 CAP Completed/Adequate?  Yes  No

Delinquent reminder notice sent: \_\_\_\_\_  
 Additional Assessment Required?  Yes  No

Remediation/Corrections: \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_