SAN BERNARDINO COUNTY
Behavioral Health
303 E. Vanderbilt Way San Bernardino | (909) 388-0900
www.SBCounty.gov

Data Sanitization Policy

Effective Date	09/25/2024
Approval Date	09/25/2024

DocuSigned by:
Dr. Georgina Yoshioka
7DF8077EFA674B2...
Georgina Yoshioka, DSW, MBA, LCSW, Director

Policy

It is the policy of the Department of Behavioral Health Information Technology (DBH-IT) department to sanitize all media, removable media, business mobile computing devices, and information assets prior to disposal, release outside of organizational control, or release for reuse, to render Electronic Protected Health Information (ePHI), personal identifying information (PII) and all other confidential data permanently non-retrievable consistent with the National Institute of Standards and Technology (NIST) Special Publication 800-88r1, REV-1 Guidelines for Media Sanitization.

Purpose

To provide instruction for establishing proper sanitization of media in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and California State laws which require ePHI to be protected from unauthorized access, use or disclosure. This policy applies to all present and future physical devices or media capable of storing ePHI data.

Data Sanitation Standards

All electronic medical records will be stored, backed up, or retained in accordance with the **Retention of Medical Records Policy** (COM0906). If media or data storage devices cannot be wiped, the device(s) must be destroyed in a manner that renders the information unrecoverable and the media device unusable.

Computer hard drives, which are to be imaged for reuse, shall also be sanitized before reimaging. Other media such as CD/DVDs, flash/USB drives, and other portable media, shall be sanitized before reuse or physically destroyed, pulverized, shredded or incinerated.

Data Sanitation Standards

In the event it is necessary to retain a vendor to sanitize media and equipment, the vendor shall be approved by the DBH Office of Compliance (Compliance) prior to accessing protected media and shall sign the DBH Oath of Confidentiality (COM027). Approved business associates will have appropriate data security safeguards in place to ensure media is secured from unauthorized access, use or disclosure in compliance with 45 CFR §164.310(d)(2)(i).

Continued on next page

Data Sanitization Policy, Continued

Responsibilities

Roles and responsibilities are outlined as follows:

Role	Responsibility
DBH Staff	• Bring media devices such as hard drives, USB sticks, CDROM's, and other data storage devices to the DBH IT department for disposal or sanitization when the media is no longer required or when requested by DBH-IT.
DBH-IT	• Ensure the sanitization process is documented in compliance with NIST sanitization certification standards. • Maintain a contemporaneous log of all disposed media devices and storage media.

Related Policies, Procedures and Forms

DBH Standard Practice Manual and Departmental Forms:

- Device and Media Controls Policy (IT5008)
- Confidentiality of Protected Health Information (PHI) (COM0905)
- Retention of Medical Records Policy (COM0906)
- Unauthorized Access of Confidential Medical Records (COM0907)
- Security of Protected Electronic Health Information Policy (COM0923)
- Data Integrity Policy (COM0925)
- Transportation of Protected Health Information (PHI) Policy (COM0948)
- Transportation of Protected Health Information (PHI) Procedure (COM0948-1)

Regulatory References

- Code of Federal Regulations, Title 45, Part 164
- Code of Federal Regulations, Title 42 Part 2, Final Rule
- NIST Special Publication 800-88r1, Guidelines for Media Sanitization