




|   |  |  |        |
|---|--|--|--------|
|  |  | <h1>Data Sanitization and Equipment Disposal Policy</h1> |        |
| Effective Date:   |  | Standard Number:   |        |
| Next Review Date:   |  | Supersedes:  |        |
| Last Updated:   |  | Page:  | 1 of 3 |

## Purpose:

To:

- ensure confidential information has been removed from company-owned electronic devices and media prior to disposal, repair or re-purposing;
- prevent data security and confidentiality from being compromised;
- ensure compliance with HIPAA standards;
- ensure compliance with environmental state and federal regulations for waste disposal.

## Scope:

All company-owned electronic devices and media, whether on or off premises, whether operated by an employee, contractor, or business partner.

## Policy:

Data contained on information system media and equipment, including PHI and confidential information, must be protected from unauthorized disclosure by sanitizing or destroying the media or equipment before disposal or reuse.



## Responsibilities

The IT Department shall be responsible for the sanitization of all electronic devices and media to eliminate opportunities for confidentiality to be compromised, prior to equipment disposal, repair or re-purposing [re-purposing includes preparing equipment for use by a different user or department, donating the equipment to a charity, or selling the equipment to an electronic equipment recycler or reseller.] Users are required to contact the IT Department when any electronic device or media needs to be disposed. Users are prohibited from disposing of media (except paper) and equipment themselves. The IT Department shall ensure that equipment and media awaiting sanitization and/or disposal is stored in a controlled-access, secured environment. The IT Department shall maintain records showing that the equipment has been properly sanitized before it is disposed or re-used. Non-compliance issues shall be brought to the attention of the Security Officer. The IT Department shall maintain the technical procedures for performing the sanitization and disposal processes, and is responsible for selection and training on the tools used for sanitization.

## Inventory Reconciliation

Before any computer or hard drive is sanitized, an inventory of any software licenses contained on it must be reconciled. If the system will be re-purposed and the software license will be re-used, no inventory adjustment is necessary. However, if the software will not be re-used, or the system is slated for disposal, the software license must be removed from inventory. Likewise, if the hardware will be disposed, its serial number must be recorded and inventory records adjusted when it is no longer on the premises. It is essential to maintain accurate hardware and software inventories for asset tracking (see *Asset Tracking Policy*), to maintain (or drop) license agreements and support contracts, and for budgetary/finance purposes.

## Computer System or Hard Disk

Before any company-owned hard disk or system containing a hard disk is transferred, donated, or disposed of in any form or fashion, it shall be "sanitized" by reformatting the hard drive in a secure manner or by using an approved low-level erasure utility that conforms to the DOD 5220-22-M standards. After sanitization, all boot-up and BIOS passwords must also be removed. If sanitization is performed by an outside party or vendor,  must be provided with the appropriate documentation of the sanitization process. If the system is being sent outside the company for repair or data recovery,  must have a chain-of-custody and non-



|                          |  |  |        |
|--------------------------|--|--|--------|
|                          |  | <b>Data Sanitization and<br/>Equipment Disposal Policy</b> |        |
| <b>Effective Date:</b>   |  | <b>Standard Number:</b>                                    |        |
| <b>Next Review Date:</b> |  | <b>Supersedes:</b>   |        |
| <b>Last Updated:</b>     |  | <b>Page:</b>   | 2 of 3 |

disclosure agreement with the organization performing the service, if the data cannot be sanitized prior to repair/recovery. If sanitization is performed in-house, a sticker shall be affixed to the computer indicating the date and initials of person who performed the wiping operation. If the disk drive is non-operational, the drive must be taken out of the computer and physically destroyed or a degausser can be used to disrupt the contents of the drive. A sticker shall be affixed on the remains of the disk drive indicating it has been destroyed, the date, and the initials of the person doing the destruction.

#### **Portable Media**

For media, such as discs, tapes, USB/flash drives, etc., as well as company-issued cell phones/PDAs, the IT Department shall see to it that all data and software has been securely removed or that the media has been rendered unusable, so that there is no possibility of data security or confidentiality breaches when media is disposed or reused. Simply deleting a file is not sufficient to prevent someone from un-deleting the file later.

#### **Equipment Disposal**

Many types of electronic equipment present a hazard if disposed of improperly due to the presence of lead and mercury. This includes cell Phones/PDAs, CRT/LCD devices, batteries, power supplies, as well as laptops and other computers. [REDACTED] shall ensure electronic equipment is disposed of in an environmentally-friendly way in accordance with state and federal EPA regulations. If the system is non-operational (for example, if the system or hard disk cannot be booted up in order to run the sanitization utility on it), the IT Department must physically destroy the hard disk or media by crushing or drilling prior to disposal. Portable media (diskettes, tapes, CD-ROMs) may be destroyed by crushing, shredding, or melting prior to disposal. Electronic equipment shall not be incinerated, as this would violate EPA guidelines. Prior to disposal, all [REDACTED]-identifiable tags should be removed from the item; stickers indicating wipe date and initials may remain. If disposal is carried out by a third-party, documentation shall be provided from them regarding the number and types of items disposed. This shall be stored with the internal list of serial numbers or inventory tag numbers corresponding to the items disposed. These items shall be deleted from inventory records as described above.

#### **Paper/Hardcopy**

Secure bins are provided in the workplace for disposing of paper containing confidential information. These bins prevent someone from retrieving previously disposed paper. The contents of these bins are shredded by a service with whom [REDACTED] has a confidentiality, chain of custody, and/or business associate agreement.

#### **Discipline**

Failure to comply with this policy may lead to disciplinary action up to and including termination. Non-compliance with state and federal laws may also lead to criminal and civil penalties.

#### **References:**

- HIPAA Security Act 164.310(d)(1) – Device and Media Controls
- HIPAA Security Act 164.310(d)(2) – Disposal, Media Re-Use, Accountability
- CMS Security Standard: Media Protection (MP)
- NIST Publication SP800-88 - Media Sanitization
- NIST Publications SP800-53, SP800-100, SP800-70
- DOD 5220-22-M Standards

**When printed, this document is uncontrolled. Please verify that you are using the most current policy or procedure based upon the controlled document on the [REDACTED] Intranet.**

|  |  |                         |
|--|--|-------------------------|
|  | <b>Data Sanitization and<br/>Equipment Disposal Policy</b> |                         |
|  | <b>Effective Date:</b>                                     | <b>Standard Number:</b> |
|  | <b>Next Review Date:</b>                                   | <b>Supersedes:</b>      |
|  | <b>Last Updated:</b>                                       | <b>Page:</b> 3 of 3     |

**REVISION HISTORY:**

| Revision | Date | Status | Responsible Party |
|----------|------|--------|-------------------|
|          |      |        |                   |
|          |      |        |                   |