Lifespan Corporation Policy	**Subject:** Media Disposal Policy	**File Under:** HIPAA Security
Issuing Department(s): Information Services		**Latest Revision Date:** July 29, 2015
Original Policy Date: October 14, 2014	**Page 1 of 4**	**Last Review Date:** July 2015
Policy Number: HSP-92.1		**Approved By:** CISO / CIO

Media Disposal Policy

Introduction

Lifespan has adopted this Media Disposal Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

Lifespan hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs Media Disposal for Lifespan. All personnel of Lifespan must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

Assumptions

- ❑ Lifespan hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations.

- Lifespan must comply with HIPAA and the HIPAA implementing regulations pertaining to media disposal and disposition, in accordance with the requirements at § 164.310(d)(1-2).
- Media containing individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), must be completely erased, properly encrypted, or totally destroyed in its final disposition, or the data residing on such media is subject to recovery and subsequent misuse or theft.

Policy Statement

- It is the Policy of Lifespan to dispose of all media containing individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), in full compliance with all the requirements of HIPAA.
- Responsibility for proper media disposal and disposition shall reside with the Director of Data Center Operations and the Technical Services Manager, who shall develop procedures to ensure the proper disposition of all such media.
- It is the Policy of Lifespan to fully document all media disposal-related activities and efforts, in accordance with our Documentation Policy.

Definitions

- Protected Health Information (PHI): Health information, including demographic information, collected from an individual and created or received by a health provider, health plan, employer or health care clearinghouse that relates to the past, present, or future physical or mental health or condition of any individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual, that identifies an individual or there is a reasonable basis to believe the information can be used to identify the individual, and that is transmitted or maintained by electronic media or any other form or medium. PHI does not include individually identifiable health information in education records covered and protected by the Family Educational Right and Privacy Act and employment records held by a covered entity in its role as an employer.
- Sensitive information or data: Any information that may only be accessed by authorized personnel. It includes Protected Health Information, financial information, personnel data, trade secrets, and any information that is deemed confidential or that would negatively affect Lifespan if inappropriately handled.
- Media: Physical objects on which data can be stored such as hard drives, disks, CDs, tapes, paper, and other storage devices.
- Transfer: To transmit ongoing use of media and the data contained therein from one party to another party that has the appropriate authorization to access and maintain the data.
- Reallocate: To transmit ongoing use of media, not including pre-existing data, from one party within Lifespan to another party within Lifespan.
- Disposal: The permanent removal of media as a Lifespan information asset.
- Authorized Personnel: Persons appointed or given authority by Lifespan Administration to take a given action or serve in a given role.
- Secure Disposal Vendor: A third party contracted to sanitize media on the behalf of Lifespan Covered Entities. Media to be sanitized shall be placed in the vendor's specially marked containers. Note: Lifespan's various secure disposal vendors have specific guidelines regarding the amount of non-paper products that may be placed in the vendors' containers. Contact the Director of Data Operations for details on the handling of non-paper media for your area.
- Clean: To render information on media inaccessible, unless special software or techniques are used. Some examples include formatting and re-imaging media.
- Sanitize: To expunge data from media or to render it in such a state that recovery of said data is reasonably impossible. Formatting and re-imaging the media are not acceptable forms of

sanitization. The use of overwriting software in accordance with provisions in this standard is an acceptable form of sanitization.

- Physical Destruction: To render media in such a state that recovery of information from the media is reasonably impossible. This is a form of sanitization. Some examples include pulverizing, mangling, and the use of an appropriate shredder. A secure disposal vendor may also be used.
- Damage: To render media in such a state that it cannot be accessed by standard methods. However, data on the media may be accessed using special techniques. For example, bending a disk such that it cannot be read by the drive does not comply with provisions in this standard. Damaging media is not an acceptable form of sanitization.
- Secure Location: An area or place with restricted and monitored access.

Procedures

- All destruction/disposal of PHI media will be done in accordance with federal and state laws and regulations and pursuant to Lifespan's written retention policy/schedule. Records that have satisfied the period of retention will be destroyed/disposed of in an appropriate manner.
- Records involved in any open investigation, audit or litigation should not be destroyed/disposed of. If notification is received that any of the above situations have occurred or there is the potential for such, the record retention schedule shall be suspended for these records until such time as the situation has been resolved. If the records have been requested in the course of a judicial or administrative hearing, a qualified protective order will be obtained to ensure that the records are returned to the organization or properly destroyed/disposed of by the requesting party.
- Sensitive information shall not be removed from its designated Lifespan area without the approval of Lifespan Management.
- Any reallocation or disposal activity that endangers the well-being of personnel or that may negatively affect Lifespan is strictly prohibited. This includes, but is not limited to, the incineration of media in the work place.
- Media shall be cleaned or sanitized only by authorized personnel.
- Media containing non-sensitive information shall be cleaned or sanitized prior to being reallocated.
- Media containing sensitive information shall be sanitized prior to being reallocated.
- Equipment containing mass storage devices, either removable or non-removable media (including hard disks, floppy disks, flash memory, optical discs, magnetic tape, etc.), with sensitive data shall be reasonably secured at all times to reduce the risk of data and equipment loss.
- Unused equipment containing mass storage devices (including desktop and laptop computers, servers, printers, copiers, fax machines, biomedical equipment, cameras, smartphones (e.g., IPhone, Blackberry), etc.) that is slated for disposal or reallocation shall be sanitized and processed as soon as possible to reduce the risk of data and equipment loss.
- A log shall be kept of all property/equipment in which media resides. The log shall include information to verify sanitization or destruction of the media.
- Sanitization methods include:
    - Use of overwriting software to expunge all data from the media.
    - Physically destroying the media.
    - Use of a degausser to reduce the magnetic flux of the media to virtually zero, thereby expunging all data from the media. The degausser used shall be appropriate for the media being sanitized.
- Media containing sensitive information shall not be placed in the regular trash unless the media is sanitized first.
- Secure disposal vendor services shall only be used for the disposal of sensitive information.
- Non-sensitive media shall be turned into the Director of Data Center Operations or the Technical Services Manager for proper disposal.
- Lifespan employees, vendors, and contractors shall report policy violations to the Office of the CISO.

- Lifespan employees who do not follow the above standards may be subject to disciplinary action up to and including dismissal.
- Vendors or contractors who do not follow the above standards may be subject to breach of contract penalties.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with Lifespan's Sanction Policy.