**Data Destruction Policy**

1. **INTRODUCTION:**

As one of the leading providers of healthcare goods and services in the region, we all must abide by various compliance regulations. The nature of our work qualifies Sprenger as a covered entity under HIPAA, as well as HITECH and HITRUST. Each member of our team on a daily basis handles Personally Identifiable Information (PII) and Protected Health Information (PHI); as such, we must abide by regulations with regard to the destruction and disposal of this information.

For further details on the definition of PII and PHI, refer to the “*PII & PHI – Enterprise Data Classification*” policy located within EPIC in the Knowledge Management portal.

Sprenger management worked together closely in designing this policy to educate staff and stakeholders of the processes in destroying PII and PHI and the potential ramifications and societal impact if such processes are not followed.

The “Enterprise – Data Destruction Policy – PII/PHI” was established to accomplish the following:

* Educate staff on common definitions and terms as it relates to PII and PHI
* Educate staff about how to appropriately destroy/dispose of PII and PHI
* Dictate roles and responsibilities of all staff when destroying/disposing of PII and PHI
* Identify specific types of PII and PHI
* Reference material for the appropriate destruction of PII and PHI
* Establish internal controls to manage the risk associated with inappropriate destruction of PII and PHI and the staff champions to seek for guidance
* Oversight structure of the policy
* Educate staff on third-party vendor management and vendor responsibility as a business associate of a covered entity
* Provide internal and external resources for further details and guidance with regard to PII and PHI
1. **DEFINITIONS:**

In order to provide a single definition of key terms, this section will clearly define key terms used throughout this policy as well as terms that can be readily identified by all Sprenger personnel and stakeholders. These key terms are adjusted to be specific to Sprenger. Whole definitions as prescribed in guidance from The Department of Health and Human Services can be found in the “Internal and External Resources” section of this policy.

|  |
| --- |
| KEY TERMS |
| Personally Identifiable Information (PII) | Any data that could potentially identify a specific individual who consumes any healthcare goods and services. This data can be sensitive or non-sensitive in nature. |
| Protected Health Information (PHI) | Any data that refers to patient data with regard to demographics, medical information, test and laboratory results, insurance information, diagnostics and any other data that a healthcare professional could potentially collect to identify an individual and determine care. |
| Health Insurance Portability and Accountability Act (HIPAA) | A law designed to provide privacy standards to protect patients’ medical records and other health information provided to health plans, doctors, insurers, hospitals and other providers of healthcare goods and services. |
| Health Information Technology for Economic and Clinical Health Act (HITECH) | A law designed to stimulate and govern the meaningful use of electronic health records (EHR). |
| Health Information Trust Alliance (HITRUST) CSF | The Health Information Trust Alliance (HITRUST) exists to ensure that information security becomes a core pillar of, rather than an obstacle to, the broad adoption of health information systems and exchanges. |
| Degauss | A method of using a strong magnet to destroy data on magnetic storage tapes such as hard drives, USB (thumb drives), smart phones or floppy disks. |
| Zeroization | A method or destroying data from electronic storage devices. This is the process of replacing all data written onto a device with zeroes or null values. |
| Covered Entity | Any organization or corporation that directly handles PHI.  |
| Business Associate | Any person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a covered entity. |

1. **SCOPE:**

 These policies and all policies referred to within are applicable to all employees, personnel, eligible providers, eligible hospitals, all business associates and other covered entities that, at any point, refer to or handle PII/PHI data whether logical or physical in nature. Under no exception is any individual who handles or comes in contact with PII/PHI or other sensitive information exempt from these policies.

1. **TYPES OF PII/PHI:**

 Instances of PII and PHI occur when we initiate the intake process for care or research purposes and gather information about a specific individual or relatives, employers or household members of the individual. (1) The scope of the information gathered can be, but is not limited to the following:

1. The individual’s past, present or future physical or mental health or condition;
2. The provision of health care to the individual, or;
3. The past, present, or future payment for the provision of health care to the individual that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. (2)

HIPAA provides 18 identifiers of PHI that are consistent with PII protected by federal and state laws and regulations. The key distinction between PII and PHI is the inclusion of medical-related information in PHI such as medical record numbers or labels on specimens obtained for care or research purposes. (3) Refer to *Table A: Examples of PII and PHI Identifiers*.

**Table A: Examples of PII and PHI Identifiers**

|  |  |
| --- | --- |
| Protected Health Information (PHI) Examples(4) | Personally Identifiable Information (PII) Examples(5) |
| * Names
* Addresses
* All elements of dates except year
* Telephone numbers
* Fax numbers
* Email addresses
* Social security numbers
* Medical record numbers
* Health plan beneficiary numbers
* Account numbers
* Certificate/license numbers
* Vehicle identifiers and serial numbers, including license plate numbers
* Device identifiers and serial numbers
* Web Universal Resource Locators (URLs)
* Internet Protocol (IP) address numbers
* Biometric identifiers, including finger and voice prints
* Full face photographic images and any comparable images
* Any other unique identifying number, characteristic, or code
 | * Names
* Addresses
* Dates such as date of birth
* Telephone numbers including mobile, business, and personal numbers
* Fax numbers
* Email addresses
* Social security numbers, passport numbers, or  taxpayer identification numbers
* Patient identification numbers
* Financial accounts or credit card numbers
* Driver’s license numbers
* Vehicle registration numbers or title numbers
* Media Access Control (MAC) addresses
* Internet Protocol (IP) address numbers
* Biometric images or template data such as fingerprints, retina scans, voice signatures, facial geometry
* Photographic images
* Information about an individual that is linked or linkable to one of the above
 |

Sprenger accepts payments from medical-related savings accounts. Additional examples of PHI include Flexible Spending Account (FSA) numbers and Health Savings Account (HSA) numbers.

1. **APPROPRIATE DISPOSAL OF PII/PHI:**

 In accordance with *45 CFR 164.520(c)* HIPAA requires that covered entities apply appropriate administrative, technical, and physical safeguards to protect the privacy of PHI, in any form. As such, Sprenger implements reasonable safeguards to limit incidental, and avoid prohibited, uses and disclosures of PHI, including in connection with disposal of such information. Refer to the “*Controls*” section of this document to validate the internal controls in place around the administrative, technical and physical safeguards of PHI. It should be noted that all Sprenger personnel and business associates must receive training on and follow the disposal policies and procedures:

* **Branded/Non-Branded PHI (Hard Copy Format):**
	+ Under federal guidelines all PHI in this format must be rendered essentially unreadable, indecipherable and otherwise cannot be reconstructed.
	+ Under this guidance the only acceptable forms of destruction are burning, pulping and pulverizing records in a controlled environment.
* **Labeled Prescription Bottles:**
	+ Sprenger users a covered business associate, “Shred-It” to pick-up, on a weekly basis, to dispose of or otherwise destroy PHI. It should be noted that Shred-It is retained via a signed business associate contract and has a current signed Master Service Agreement. Shred-It also provides an annual SOC1 around their internal controls to provide to external auditors. Call internal audit for the above mentioned documents (x21575).
* **PHI on Electronic Media:**
	+ Under federal guidelines all electronic PHI must be rendered irrecoverable, unreadable, indecipherable or otherwise logically or physically destroyed.
	+ Physical Destruction:
		- Under physical circumstances the hard copy destruction processes apply.
	+ Clearing (Zeroization):
		- Sprenger retains software to overwrite media with non-sensitive data and is to be used in the destruction of PHI.
	+ Purging:
		- Release all PHI that is to be disposed of to Sprenger IT (Building 3 Room 911A) to degauss the media.
1. **CONTROLS:**

In accordance with *45 CFR 164.520(c)* HIPAA, Sprenger Internal Audit department as well as management has developed internal controls around the destruction of PII/PHI data in accordance with guidelines set forth above.

 The internal operational controls in place at Sprenger that set forth the processes personnel must abide by when disposing of PII and PHI can be found in detail from our internal audit department. On an annual basis Sprenger hires an external auditor that performs attestation work providing stakeholders reasonable assurance that Sprenger, its personnel, and its business associates are compliant with statutory requirements in addition to policies, procedures and processes governing the destruction of data.

 For additional information or copies of reports and controls please contact Internal Audit:

 Sprenger Health Care Systems

c/o Internal Audit

 243 Hospital Way

 Dallas, PA. 18969

 263-952-1575

 SprengerAuditors@SPHospital.org

1. **POLICY OVERSIGHT:**

The oversight of and the authorizing signatory whom attests to the fact that Springer Health Care Systems abides by and remains compliant with all federal guidelines with regard to PII and PHI and its destruction rests with Sprenger CIO, Randy Halberson. PII/PHI is regulated by HIPAA with additional guidance and best practices denoted by HITRUST and HITECH. Sprenger’s policy has been crafted specifically with these regulations and guidance in mind to provide assurance to stakeholders of the proper handling of all covered data. The policy is directly enforced by:

 Randy Halberson, CIO of Sprenger Hospital

 243 Hospital Way

 Dallas, PA. 18969

 263-952-4558

 Randy.Halberson@SPHospital.org

 If Sprenger fails to comply with statutory requirements, it may be subject to fines, legal fees and lawsuits. Employees who violate this policy may be prohibited from the handling of any protected information, suspended, terminated from the company and/or having their licensure to perform services in a clinical environment revoked.

 In any situation where the policy overseer fails to enforce the policy, he/she will be promptly relieved of his/her responsibilities as oversight and face suspension or termination from the company.

1. **OUTSIDE VENDOR STATEMENT OF WORK:**

All outside or third-party vendors used by Sprenger in the handling and destruction of PHI must meet the following guidelines:

* Must have a signed statement of work prior to performing any and all services.
* In addition to a statement of work, the vendor must have a signed business associate contract; such contract must include the following sub-sections:
	+ Introduction defining a business associate
	+ Clearly articulated definition of a covered entity and the HIPAA rules
	+ Obligations and activities of the business associate
	+ Permitted users and disclosures of the business associate
	+ Provisions for covered entity to inform business associate of privacy practices and restrictions
	+ Permissible requests by covered entity
	+ Term and Termination Language
	+ An optional miscellaneous section providing option guidance on regulatory references, amendments and interpretations

For further information please refer to HIPAA Guidance: *45 CFR 164.502(e); 164.504(e); 164.532(d) and (e).*

Additionally, please call our legal and compliance office at (x21607).

**ANNUAL POLICY REVIEW AND REVISION LOG**



1. **EXTERNAL RESOURCES:**

To learn more about HIPAA and other federal laws guiding this policy, please refer to the resources listed in Table B: *Guidance Documents for Data Destruction Policy.*

**TABLE B: GUIDANCE DOCUMENTS FOR DATA DESTRUCTION POLICY**

|  |  |  |
| --- | --- | --- |
| **Source** | **Resource**  | **Link** |
| Federal Government | HIPAA Policy | <http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl> |
| HHS | HIPAA Administrative Simplification  | <http://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf> |
| HHS | Guidance on Research Using Coded Private Information or Specimens | <http://www.hhs.gov/ohrp/regulations-and-policy/guidance/research-involving-coded-private-information/> |
| NIST | Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)  | <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf> |
| NIST | Guidelines for Media Sanitization | <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf> |

**Citations:**

(1 & 2) Department of Health and Human Services: <http://www.hhs.gov/ocio/policy/>

(3) Department of Health and Human Services: <http://www.hhs.gov/ohrp/regulations-and-policy/guidance>

(4) 45 CFR 164.514 <http://www.ecfr.gov/cgi-bin/textidx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl>

(5) NIST <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>