1. **EXECUTIVE SUMMARY**

Sprenger Healthcare Systems (Sprenger) deals heavily with protected internal and external client data. This data ranges from non-sensitive to confidential and includes PHI/PII which is protected by law under HIPAA and other regulations. In order to ensure the proper destruction of this data, Sprenger has implemented a data destruction policy. This document establishes the internal auditing process that will be used to confirm the successful execution of the data destruction policy throughout the company. Internal auditing is Sprenger's effort to ensure due care regarding data destruction and is an administrative control that helps our entity prepare for annual audits conducted by external auditors.

1. **SCOPE**

This policy empowers designated internal auditing authorities to evaluate any department deemed relevant to Sprenger’s data destruction policies, including, but not limited to: IT, Finance, Accounting, and Human Resources. All data, regardless of storage format, is subject to this audit. Additional entities that may be audited include, but are not limited to: employees, vendors, contractors, or any other entity whose responsibilities include, in any way, the handling of Sprenger’s client data. An information manager should accompany the auditor throughout the process in order to ensure the auditor receives the necessary assistance and compliance from the relevant staff.

1. **OBJECTIVES**

Sprenger is dedicated to ensuring the proper handling and protection of all of our clients' data. Our auditing procedures for data destruction are a testament to this dedication. By implementing this policy we hope to ensure:

* Patient information is properly classified and handled accordingly,
* Data is destroyed in a timely manner following the expiration of its corresponding retention period, and
* Data is destroyed through the proper mediums according to its classification
1. **APPROACH**

Our approach to an internal audit of the data destruction policy is to:

* Evaluate applicable federal, state, and local laws
* Review the corporate data destruction policy and procedures and any instances of the policy and procedures modified to fit specific departments
* Conduct interviews with data owners, holders, and users including but limited to internal employees and external vendors
* Test a sample of users across the organization
* Review a sample of terminated users
1. **CONSIDERATIONS**

 Per the recommendations of NIST SP 800-88r1, Sprenger utilizes certificates of destruction. Our tool is certificate management software from vendor D2 Systems that Sprenger maintains in-house. Our understanding is that:

* The software provides serial numbers and bar codes assigned to instances of PHI/PII
* Employees and vendor representatives input updates to the status of PHI/PII such as active, inactive, pending destruction, etc.
* The software maintains running records of internal and external certificates of destruction based on employee and vendor representative input updates
* The software generates final internal certificates of destruction managed by Sprenger records management
* The software provides view-only permissions for final external certificates of destruction managed by the Sprenger vendor management/contracts team
* Third-party vendor Shred-It provides final external certificates of destruction
1. **AUDIT PLAN**

|  |  |  |  |
| --- | --- | --- | --- |
| **Audit Goal** | **Assumptions** | **Audit Review** | **Information Source** |
| Ensure that enterprise data destruction policy adheres to applicable federal, state, and local laws | The Sprenger CIO and Sprenger Compliance office update the policy when laws change  | Existing data destruction policy juxtaposed to federal, state, and local laws | Auditors will develop a compliance matrix of applicable federal, state, and local laws and existing data destruction policy |
| Ensure that physical PHI/PII is incinerated  | Sprenger employees and vendors are trained on proper handling and destruction of PHI/PII | Employee and Vendor Representatives | Auditors will interview employees with varied levels of responsibility from different departments and vendors |
| Sprenger employees do not improperly dispose of PHI/PII | Employee and/or building waste receptacles | Auditors will obtain waste receptacles independently |
| Termination procedures for Sprenger employees includes PHI/PII destruction | Terminated employee  | Auditors will review out-processing documentation for a sample of terminated employees |
| Sprenger employees utilize enterprise software for tracking the creation and destruction of PHI/PII | Internal Certificates of Destruction  | Auditors will retrieve internal certificates of destruction from the Sprenger records management database and/or hard copy files |
| Sprenger employee utilize third-party vendor Shred-It for final PHI/PII destruction | External Certificates of Destruction | Auditors will retrieve external certificates of destruction from the vendor management/contracts team |
| Ensure that deleted PHI/PII cannot be recovered | Sprenger employees and vendors are trained on proper handling and destruction of PHI/PII | Employee and Vendor Representatives | Auditors will interview employees with varied levels of responsibility from different departments and vendors |
| Termination procedures for Sprenger employees includes PHI/PII destruction | Terminated employee  | Auditors will review re-shelved equipment previously assigned to a sample of terminated employees and confirm account terminations for storage containing PHI/PII |
| Sprenger employees do not improperly dispose of PHI/PII | Workstation hard drives | Auditors will review a random sample of workstation hard drives |
| Server hard drives | Auditors will review a random sample of server hard drives |
| Cloud-based software storage | Auditors will review three cloud-based software storages |
| Mobile and handheld devices | Auditors will review five random samples of mobile and handheld devices |
| Ensure that prescription bottles are all located within the proper Shred-It receptacles and that those receptacles are locked and maintained in a secure location | Sprenger employees and vendors are trained on proper handling and destruction of PHI/PII | Employee and Vendor Representatives | Auditors will interview employees with varied levels of responsibility from different departments and vendors |
| Sprenger employees do not improperly dispose of PHI/PII | Employee and/or building waste receptacles | Auditors will obtain waste receptacles independently |
| Internal Certificates of Destruction | Auditors will retrieve internal certificates of destruction from the Sprenger records management database and/or hard copy files |
| Sprenger employee utilize third-party vendor Shred-It for final PHI/PII destruction | External Certificates of Destruction | Auditors will retrieve external certificates of destruction from the vendor management/contracts team |
| Ensure that all information is deleted within 10 days following the expiration of the retention period | Sprenger employees and vendors are trained on proper handling and destruction of PHI/PII | Employee and Vendor Representatives | Auditors will interview employees with varied levels of responsibility from different departments and vendors |
| Sprenger employees do not improperly dispose of PHI/PII | Internal Certificates of Destruction  | Auditors will retrieve internal certificates of destruction from the Sprenger records management database and/or hard copy files |
| Sprenger employee utilize third-party vendor Shred-It for final PHI/PII destruction | External Certificates of Destruction | Auditors will retrieve external certificates of destruction from the vendor management/contracts team |

1. **COMMUNICATION PLAN**

Before June 1: An audit will take place without verbal or written communication any day to evaluate policy controls and behavioral adherence under normal operating conditions. This is consistent with external auditing and helps maintain integrity in Sprenger’s auditing processes.

One Week Post-Audit: Internal auditors will communicate efficiency, deficiency, and action plans for any remedial action.

Two Weeks Post-Audit: Action plan response from any deficient employee or group such as a department is due and allows stakeholders to identify any barriers to policy adherence or remedial action.

Three Weeks Post-Audit: Action plan deliverables from any deficient employee or group such as a department is due. At this point, deficiencies should be rectified or executive management should have clear documentation for why Sprenger is unable to rectify a specific deficiency.