Paper Destruction Policy

**Purpose**

It is the policy of [Insert Covered Entity or Business Associate name] to ensure the privacy and security of protected patient health information (PHI) in the maintenance, retention, and eventual destruction/disposal of such media.

**Definitions**

1. Protected Health Information (PHI): 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.
2. Sanitization: Removal or the act of overwriting data to a point of preventing the recovery of the data on the device or media that is being sanitized. Sanitization is typically done before re-issuing a device or media, donating equipment that contained sensitive information or returning leased equipment to the lending company.

**Policy**

1. All destruction of PHI will be done in accordance with federal and state laws and regulations and pursuant to [Insert Covered Entity or Business Associate name] written retention policy. Records that have satisfied the period of retention will be destroyed of in an appropriate manner.
2. Records involved in any open investigation, audit or litigation should not be destroyed. In the event such exception occurs, the record retention schedule shall be suspended until the situation has been resolved. Exceptions where records are leaving the organization premises require a protective order to ensure the records are returned to the organization.
3. Records scheduled for destruction should be secured against unauthorized access until the destruction of PHI is complete. Paper media containing confidential data shall be kept in locked bins until destruction.
4. A record of all PHI destruction must be retained by the organization. The organization has the burden of proof for any PHI destruction, regardless of whether destruction is done by the organization or a contractor. It may be necessary to prove that the records were destroyed during the regular course of business. Records of destruction, such as a certificate of destruction, should include:
   1. Date of destruction.
   2. Method of destruction.
   3. Description of the destroyed record series or medium.
   4. Inclusive dates covered.
   5. A statement that the patient records were destroyed in the normal course of business.
   6. The signatures of the individuals supervising and witnessing the destruction.
5. Copies of documents and images that contain PHI that are not originals do not require retention based on retention policies. Copies shall be destroyed by shredding or other acceptable manner as outlined in this policy. Certification of destruction is not required.
6. The methods of destruction should be reassessed periodically, based on current technology, accepted practices, and availability of timely and cost-effective destruction technologies and services.
7. Business Associates
   1. If destruction services are contracted, the contract must provide that the organization’s business associate will establish the permitted and required uses and disclosures of information by the business associate as set forth in the federal and state law (outlined in [Insert Covered Entity or Business Associate name] HIPAA Business Associated Agreement).
   2. The business associate agreement must provide that, upon termination of the contract, the business associate will return or destroy of all patient health information. If such return or destruction is not feasible, the contract must limit the use and disclosure of the information to the purposes that prevent its return or destruction.
   3. The Business Associate Agreement should also set minimum acceptable standards for the sanitization of media containing PHI. The Business Associate Agreement should include but not be limited to the following:
      1. Specify the method of destruction.
      2. Specify the time that will elapse between acquisition and destruction of data/media.
      3. Establish safeguards against unauthorized disclosures of PHI.
      4. Indemnify the organization from loss due to unauthorized disclosure.
      5. Require that the business associate maintain liability insurance in specified amounts at all times the contract is in effect.
      6. Provide proof of destruction (e.g. certificate of destruction).

**Violations:**

Any individual, found to have violated this policy, may be subject to disciplinary action up to and including termination of employment. Violations shall be noted in the [Insert Covered Entity or Business Associate name] issue tracking system and support teams shall be dispatched to remediate the issue.