**Media Sanitization and Disposal Policy**

**PURPOSE:**

Trialomics, Inc is committed to complying with HIPAA Security Rule requirements pertaining to the integrity, confidentiality, and availability of electronic protected health information. Trialomics, Inc recognizes there are times in which media will need to be destroyed. This policy has been created to effectively destroy media while adhering to the HIPAA Security rules.

**POLICY:**

Trialomics, Inc requires all ePHI are never stored outside the AWS cloud. Upon termination of our relationship with a covered entity, records in the cloud environment containing ePHI will be securely overwritten and such steps taken will be documented.

**DEFINITIONS:**

1. Electronic Protected Health Information (ePHI): Individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.
2. Securely Overwritten: The process of overwriting data with 1 and 0 to render the data irretrievable.
3. Physically Destroyed: The process of physically destroying electronic media to an extent where data is no longer retrievable.
4. Reuse of Hardware: The process of reallocating hardware that contains or may have contained ePHI to an individual that does not have authority to access ePHI.
5. Degauss: Using a magnetic field to erase (neutralize) the data stored on magnetic media.
6. 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 contains sensitive information, or returning leased equipment to the lending company.

**PROCEDURE:**

1. No media or devices will be reused.
2. All destruction/disposal of patient health information media will be done in accordance with federal and state laws and regulations and pursuant to the organization’s written retention policy/schedule. Records that have satisfied the period of retention will be destroyed/disposed of in an appropriate manner.
3. 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.
4. All original ePHI must be backed up on a regular basis. Backup mechanisms will be tested regularly to verify that ePHI can be efficiently retrieved. Backups of original ePHI are stored in distinct geographic locations.
5. Copies of documents and images that contain PHI and are not originals that do not require retention based on retention policies (e.g., provider copies, schedule print outs etc.) shall be destroyed/disposed of by shredding or other acceptable manner as outlined in this policy. Certification of destruction is not required.
6. Records scheduled for destruction/disposal should be secured against unauthorized or inappropriate access until the destruction/disposal of PHI is complete.
7. A record of all PHI media sanitization should be made and retained by the organization. The organization has the responsibility to retain the burden of proof for any media destruction regardless of whether destruction is done by the organization or by a contractor. Retention is required because the records of destruction/disposal may become necessary to demonstrate that the patient information records were destroyed/disposed of in the regular course of business. Records of destruction/disposal, such as a certificate of destruction, should include:
   1. Date of destruction/disposal.
   2. Method of destruction/disposal.
   3. Description of the destroyed/disposed record series or medium.
   4. Inclusive dates covered.
   5. A statement that the patient information records were destroyed/disposed of in the normal course of business.
   6. The signatures of the individuals supervising and witnessing the destruction/disposal.