**Data Backup Policy**

**Purpose:**

This policy reflects Trialomics, Inc commitment to backup and securely store all ePHI on its information systems and electronic media.

**Policy:**

1. The Information Security Officer will be responsible for implementing this policy and will ensure that further responsibility is properly assigned for the proper management of data.
2. The Information Security Officer or designee is responsible for ensuring effective training of the workforce members assigned to complete backups, for management of the backup media and for performing periodic testing of restored media.
3. Data Backup
   1. In order to protect the confidentiality, integrity, and availability of ePHI, Trialomics, Inc completes backups as follows:
      1. RDS: Backups are stored for each of the last 7 days and multi-az deployment is used to ensure high availability and failover support.
      2. Elasticsearch: Backups are stored hourly for the past 14 days in S3.
      3. S3: objects are redundantly stored on multiple devices across multiple facilities in an Amazon S3 Region.
   2. All data backup systems are automated.
      1. Automated systems electronically capture backup locations, date/time, and ensure encryption and restricted access.
   3. Stored data is accessible and retrievable at all times, except in the event of a catastrophic event at an Amazon data center.
   4. Documentation of backup restoration events are maintained and capture the date and time the data was restored.
   5. Operational procedures for backup, recovery, and testing are documented and periodically reviewed as described in the Contingency Plan.
4. Destruction
   1. Trialomics returns all records to corresponding covered entities within 30 days of the termination of our contract.
   2. Once the covered entity confirms receipt of the data, Trialomics deletes all stored copies in the AWS accounts, including the databases and servers used to store the data.