**Integrity Controls Policy**

**PURPOSE:**

Trialomics, Inc, which handles ePHI, will implement the ability to authenticate, which is the process used to validate data integrity, to verify that the data sent is protected against unauthorized alteration or destruction during transmission over electronic communications networks.

**POLICY:**

1. The Security Officer will approve the electronic mechanisms that will be implemented to protect ePHI from unauthorized alteration or destruction and to authenticate the integrity of ePHI during transmission.
2. The Security Officer will determine the appropriate steps to confirm effective implementation of the integrity controls, to review and update them as necessary as defined by the Evaluation policy.
3. The Security Officer will provide affected workforce members with training and awareness regarding integrity controls implemented to protect ePHI from unauthorized alteration or destruction during transmission over electronic communications networks.
4. The Security Officer will ensure that actual and potential damage to the integrity of confidential or sensitive information, including ePHI, is appropriately addressed.
5. Transmitting ePHI will never occur via email or a removable media such as a flash drive or removable hard drive.
6. The Security Officer will ensure an adequate firewall protection of the network.
   1. The firewall shall be configured to “deny” rather than “allow” as the default setting.
   2. Unused firewall ports shall be closed.
   3. AWS Config will be used to constantly monitor firewall and security configurations and alert the Security Officer via SMS and/or Email
7. All encryption mechanisms utilized for transmission of ePHI will support a minimum of 128 bit encryption.
8. The following provides the mechanism to corroborate that ePHI has not been altered or destroyed in an unauthorized manner:
   1. All versions of all ePHI data are stored as S3 objects which can neither be modified or deleted, ensuring an audit trail that includes who modified which data and when.
   2. All ePHI data stored in S3 will be modified (created or updated) only by the API application running on the EC2 servers or via clients using presigned URLS generated by the API application.
   3. To support client applications that read and write ePHI, the same API will store the latest data versions across multiple database technologies. These applications connect to the Picard API which handles authenticating and coordinating the flow of data and requests across different cloud services.
   4. All API requests are logged with information about who made what request when, providing another means of ensuring data integrity and provenance.
   5. Creating or updating ePHI via the API requires a valid session which requires a username and password. Users who are reading or writing ePHI also must be part of the appropriate system Role(s) and only Administrators can add/remove this Role(s).