**Encryption Policy**

**Purpose:**

The goal of these policies is to protect patient health information and other protected information such as individually identifying information by enhancing the security of our electronic information systems. Trialomics, Inc requires all Protected Health Information (PHI) to be located in Amazon Data Centers. Amazon Data Centers have had a formal risk assessment on the physical and logical controls with no findings that would render the data center unsecured.

These policies and guidelines apply to all workforce members who use, collect and/or access PHI. These policies and guidelines apply to all Trialomics, Inc owned and personal electronic devices that are connected to Trialomics, Inc networks and receive, store or transmit PHI.

**DEFINITIONS:**

1. Encryption: the process of converting data to an unrecognizable or "encrypted" form.
2. Protected Health Information (PHI): Individually identifiable health information transmitted or maintained in any form.
3. Electronic Protected Health Information (ePHI): Individually identifiable health information transmitted or maintained in electronic form.
4. Workforce Member: Employees, volunteers (board members, community representatives), trainees (students), contractors and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

**Policy:**

1. The Information Security Officer will provide appropriate workforce members with training and awareness regarding encryption methods implemented to protect ePHI from unauthorized alteration or destruction during transmission over electronic communications networks (see “[Security Training: Program Policy & Procedures for Information Security Officer](https://docs.google.com/document/d/1ojC9U92vU94-9QTuAJ0JaO8_xQjAAqlVI9HsWMTgJGU/edit)”).
2. All encryption of AWS services utilizes AWS KMS.
3. All ePHI will never be saved to disk on any mobile media, laptops, workstations, or servers outside of the corresponding AWS account.
4. All ePHI will be encrypted, whether at rest or in transmission, where a risk analysis indicates that such encryption is necessary to protect the security of PHI. Please see the Risk Management Policy and Procedure for more details.
5. All electronic devices that receive and/or transmit PHI and are not located in AWS Data Center must use approved encryption methods to secure the information stored on or transmitted outside the secure clinical network.
6. Files or text that contain PHI will never be transmitted across the Internet using e-mail.

**Exceptions:**

Existing systems and applications containing Protected Information which cannot use encryption because of a technological limitation, but have compensating controls, may be granted a special exception by the Information Security Officer. However, these systems and applications will be required to have a formal risk assessment performed by the Information Security Officer to ensure that major risks are addressed via compensating controls to protect the data in lieu of encryption. Exceptions will be reviewed periodically and removed when a suitable solution is available.