**Person or Entity Authentication**

**PURPOSE:**

The purpose of this policy is to comply with the HIPAA Security Rule’s requirements pertaining to the integrity, confidentiality, and availability of electronic protected health information (ePHI). The Person or Entity Authentication Standard of the Rule requires covered entities to implement policies and procedures to validate user or entity identification prior to permitting access to ePHI to those individuals or groups authorized, thereby increasing the security of ePHI.

**SCOPE:**

This policy covers all ePHI, which is available currently, or which may be created, used in the future. This policy applies to all workforce members who collect, maintain, use, or transmit ePHI in connection with activities at Trialomics, Inc.

**POLICY:**

1. To ensure that all individuals or entities that access ePHI have been appropriately authenticated, the following procedures must be implemented:
   1. All persons or entities that have the need to access confidential or sensitive data, including ePHI, from information systems must first be authorized to access that data before having an account established on any information system. In addition, whenever a person or entity is authorized to access such information, only the minimum necessary to perform their designated function is to be authorized for access.
   2. Workforce members seeking access to any network, system, or application that contains ePHI must satisfy a user authentication mechanism such as a unique user identification and password, biometric input, or a user identification smart card to verify their authenticity.
   3. Workforce members seeking access to any network, system, or application must not misrepresent themselves by using another person’s User ID and Password, nor other authentication information.
   4. Workforce members are not permitted to allow other persons or entities to use their unique User ID and password, smart card, or other authentication information.
   5. A reasonable effort must be made to verify the authenticity of the receiving person or entity prior to transmitting ePHI.
2. Network users are responsible for adhering to this policy. Administrators of systems that maintain PHI are responsible for ensuring the policies statements detailed above are implemented on all systems that store, transmit, or maintain PHI.
3. The Information Security Officer is responsible for verifying that an authentication mechanism on systems that store, transmit, or maintain PHI are functional, appropriate and reasonably mitigate the risk of unauthorized access.
4. The Information Security Officer shall take reasonable and appropriate steps to ensure that workforce members are provided training and awareness about the authentication methods used by Trialomics, Inc.

**PROCEDURE:**

1. Trialomics, Inc authentication processes include:
   1. Uniquely identifiable authentication identifiers in order to track the identifier to a workforce member.
   2. Use of MFA to access AWS accounts.
   3. Use of SSH keys to access EC-2 servers.
   4. Confirmation through a company managed account that user HIPAA security training certification is up to date.
   5. The ISO will add new accounts after confirming the HIPAA certification status and ensuring the user has an MFA device.
   6. The ISO will remove or disable authentication credentials in ePHI Systems for persons or entities that no longer require access to ePHI as soon as they are notified.
   7. Periodic validation that no redundant authentication credentials have been issued or are in use.
   8. Protection of authentication credentials (e.g., passwords, PINs) with appropriate controls to prevent unauthorized access.
   9. When feasible, masking, suppressing, or otherwise obscuring the passwords and PINs of persons and entities seeking to access ePHI so that unauthorized persons are not able to observe them
2. Trialomics, Inc shall limit authentication attempts to its ePHI to no more than 1 attempt.
   1. Authentication attempts that exceed the limit will result in:
      1. Logging of event
      2. Notifying appropriate Trialomics, Inc management.

**ADMINISTRATION AND INTERPRETATIONS:**

This policy shall be administered by the Information Security Officer. Questions regarding this policy should be directed to the Information Security Officer.