**Remote Access Policy and Procedure**

**Purpose:**

To establish uniform security requirements for all authorized users who require remote electronic access to Trialomics, Inc network and information assets. The guidelines set forth in this policy are designed to minimize unauthorized use of Trialomics, Inc resources and confidential information.

**Definitions:**

1. Defined Network Perimeter: Refers to the boundaries of the Trialomics, Inc internal computer network.
2. Electronic Protected Health Information (ePHI): PHI shall have the same meaning as defined by 45 C.F.R. 160.103.
3. Firewalls: A logical or physical discontinuity in a network to prevent unauthorized access to data or resources. A firewall is a set of hardware and/or related programs providing protection from attacks, probes, scans and unauthorized access by separating the internal network from the Internet.
4. Information Resources: Networks, systems, applications, and data including but not limited to, ePHI received, created, maintained or transmitted by the Trialomics, Inc.
5. Privileged Access Controls: Includes unique user IDs and user privilege restriction mechanisms such as directory and file access permission, and role-based access control mechanisms.
6. Remote Access: The ability to gain access to Trialomics, Inc network from outside the network perimeter. Common methods of communication from the remote computer to Trialomics, Inc network includes, but is not limited to, Virtual Private Networks (VPN), web-based Secure Socket Layer (SSL) portals, and other methods which employ encrypted communication technologies.
7. Role-Based Access: Access control mechanisms based on predefined roles, each of which has been assigned the various privileges needed to perform that role. Each user is assigned a predefined role based on the least-privilege principle.
8. Web-based Portal: A secure website offering access to applications and/or data without establishing a direct connection between the computer and the hosting system. Web-based portals most often use 128-bit or higher SSL encryption.
9. 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:**

To establish guidelines and define standards for remote access to Trialomics, Inc information resources which receive, create, maintain or transmit ePHI by and for the organization. Remote access is a privilege, and is granted only to remote users who have a defined need for such access, and who demonstrate compliance with Trialomics, Inc established safeguards, which protect the confidentiality, integrity, and availability of information resources.

**Applicable To:**

All users who work outside of the organization’s environment, who connect to the organization’s network systems, applications and data, including but not limited to applications that contain ePHI, if applicable, from a remote location. Users may include members of the workforce, business associates, and vendors. These users may have permanent or temporary access, which may include temporary emergency remote access.

**Procedures:**

1. Gaining Remote Access
   1. Workforce members will be granted remote access connections at the discretion of the Information Security Officer.
   2. The workforce member is responsible for adhering to all of Trialomics, Inc policies and procedures, not engaging in illegal activities, and not using remote access for interests other than those for Trialomics, Inc.
   3. It is the user’s responsibility to ensure that the remote worksite meets security and configuration standards established by Trialomics, Inc. This includes configuration of personal routers and wireless networks.
   4. Each user must use their own account and not share accounts with other users.
2. Equipment, Software, and Hardware
   1. The organization will not provide all equipment or supplies necessary to ensure proper protection of information to which the user has access. The following assists in defining the equipment and environment required.
      1. Organization Provided:
         1. SSH Keys for EC2 server access
         2. AWS Console Log In for accessing and working with AWS services
      2. User Provided:
         1. Broadband connection and fees
         2. MFA enabled device linked to AWS account
         3. Secure office environment isolated from visitors and family
   2. Remote users will be allowed access through the use of equipment owned by or leased to the entity, or through the use of the workforce member’s personal computer system provided it meets the minimum standards developed by Trialomics, Inc, as indicated above.
   3. Remote users utilizing personal equipment, software, and hardware are:
      1. Responsible for remote access. Trialomics, Inc will bear no responsibility if the installation or use of any necessary software and/or hardware causes lockups, crashes, or any type of data loss.
      2. Responsible for remote access used to connect to the network and meeting Trialomics, Inc requirements for remote access.
      3. Responsible for the purchase, setup, maintenance or support of any equipment not owned by or leased to Trialomics, Inc.
   4. Troubleshooting of telephone or broadband circuits installed is the primary responsibility of the remote access user and their Internet Service Provider. It is not the responsibility of Trialomics, Inc to work with Internet Service Providers on troubleshooting problems with telephone or broadband circuits not supplied and paid for by Trialomics, Inc.
3. Security and Privacy
   1. Only authorized remote access users are permitted remote access to any of Trialomics, Inc computer systems, computer networks, and/or information, and must adhere to all of Trialomics, Inc policies.
   2. It is the responsibility of the Information Security Officer to ensure any successful and failed logins to the AWS account trigger automated alarms which send SMS text messages. Any login attempt that is not authorized or
   3. It is the responsibility of Trialomics, Inc workforce members with remote access privileges to the network to ensure that their remote access connection complies with the security requirements listed above.
   4. Secure remote access must be strictly controlled through strong authentication in accordance with the Password Policy.
   5. At no time should any user of Trialomics, Inc network resources provide their login or email password to anyone, not even family members. When using a shared personal computer, for example, users should employ encryption and set up separate accounts so that other users of the computer cannot access sensitive data.
   6. It is the responsibility of the remote access user, including Business Associates and contractors and vendors, to log-off and disconnect from Trialomics, Inc network when access is no longer needed to perform job responsibilities.
   7. Remote users shall lock the workstation and/or system(s) when unattended, so that no other individual is able to access any ePHI or organizationally sensitive information.
   8. It is the responsibility of remote access users to ensure that unauthorized individuals do not access the network. At no time will any remote access user provide (share) their username or password to anyone, nor configure their remote access device to remember or automatically enter their username and password.
   9. The Remote Access User must report to the Security Officer within 24 hours of any use or disclosure of PHI in a manner not permitted by this Policy or the Agreement. After the verbal report, the Remote Access User must send a written report to the Security Officer within 72 hours. The report must contain:
      1. The identification of each individual including contact information.
      2. A brief description of what happened, including the date of the unauthorized use or disclosure and the date of the discovery of the unauthorized use or disclosure, if known.
      3. A description of the types of PHI involved (such as name, Social Security number, date of birth, home address, or account number).
      4. A brief description of what the Remote Access User is doing or has done to investigate the unauthorized use or disclosure, mitigate losses to individuals, and protect against any further breaches.
      5. Identification of the names and respective titles of those who conducted the investigation on behalf of the Remote Access User.
   10. The Remote Access User must report to the Security Officer within 24 hours of any successful security incident of which it becomes aware that affects PHI.
   11. Any employee who becomes aware of an unauthorized use or disclosure by a Remote Access User must immediately contact the Security Officer.
   12. Remote access users must take necessary precautions to secure all of Trialomics, Inc equipment and proprietary information in their possession.
   13. Copying of confidential information, including ePHI, to personal media (hard drive, USB, cd, etc.) is strictly prohibited, unless the organization has granted prior approval in writing.
   14. Since online cloud services (e.g., Carbonite, Dropbox, iCloud, Mozy) may allow for data to be copied from a PHI approved network to a network not controlled by Trialomics, Inc, they are not acceptable for use. Users must consult with IT or the Security Officer for remote file storage mechanisms.
   15. Trialomics, Inc maintains logs of all activities performed by remote access users while connected to Trialomics, Inc network. The Information Security Officer is responsible for setting up and continuously monitoring an automated intrusion detection system to detect suspicious activity.
   16. Accounts that have shown no activity for 30 days will be disabled.
   17. Electronic Data Security
       1. Backup procedures have been established that encrypt data moved to an external media.
       2. Transferring data to the Trialomics, Inc requires the use of an approved SSL/TLS connection to ensure the confidentiality and integrity of the data being transmitted. Users may not circumvent established procedures when transmitting data to the Trialomics, Inc.
       3. Users may not send any ePHI via e-mail..
   18. Paper document security
       1. It is directly prohibited for remote users to use or print paper documents that contain PHI.
       2. Documents containing PHI must be shredded immediately
4. Enforcement
   1. Remote access users who violate this policy are subject to sanctions and/or disciplinary actions, up to and including termination of employment or contract. Termination of access by remote users is processed in accordance with Trialomics, Inc termination policy.
   2. Remote access violations by Business Associates and vendors may result in termination of their agreement, denial of access to the Trialomics, Inc network, and liability for any damage to property and equipment.