**Information System Activity Review Policy**

**Policy:**

Trialomics, Inc will review logs of access and activity of electronic protected health information (ePHI) applications, systems, and networks and address standards set forth by the HIPAA Security Rule to ensure compliance to safeguarding the privacy and security of ePHI. The Security Rule requires healthcare organizations to implement reasonable hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI. Review activities may be limited by application, system, and/or network reviewing capabilities and resources. Trialomics, Inc shall make reasonable efforts to maintain information privacy and security through a well-thought-out approach to reviewing activity logs, which is consistent with available resources.

**Scope:**

This policy has been developed to address the organization-wide approach to information system log review processes.

**Procedure:**

1. Responsibility for setting up and monitoring information system access and activity is assigned to the Trialomics, Inc Information Security Officer.
2. Identifying the information systems that require monitoring is carried out as part of the Risk Assessment. The results can be found in the Risk Analysis Results document.
3. Automated monitoring systems will be configured to enable real time monitoring and surveillance of each resource. The following monitoring systems are required at all times:
   1. Automated alarms within the AWS account to notify the ISO whenever any of the following occur:
      1. A failed login attempt to the AWS console.
      2. A successful login attempt to the AWS console.
      3. A server stops responding to API requests.
      4. A change is made to a security group that exposes a protected resource to someone outside the VPC.
   2. On each EC2 instance:
      1. Configure fail2ban to restart each night and send separate emails when the restart process begins and ends successfully.
      2. Configure fail2ban to notify via email whenever a server is accessed with an ssh-key.
   3. The flask app:
      1. Nightly scans of the server logs to look for EC2 server ssh-access. If any are detected then send an SMS message indicating which server was accessed. This is used to monitor logins to servers in the case the fail2ban service is not running.
4. The Information Security Officer is responsible for reviewing the sms and email messages sent by the automated monitoring systems as follows:
   1. The Information Security Officer will not document alarms that are sent in response to approved usage of the AWS account or EC2 servers.
   2. If any notifications are received and the ISO is not aware of who carried out the corresponding action, then they will immediately investigate the issue. If through this investigation they identify the issue is not of concern, then they must document the event on the Automated Monitoring Incidents worksheet in the Periodic Ledger. If the issue is concerning (meaning somebody might have gained inappropriate access to ePHI), then they must notify the Privacy Officer immediately and carry out the necessary steps to fix the issue.
5. The Information Security Officer is responsible for reviewing, at least monthly, the automated monitoring systems to ensure they are operating, and the api logs to detect any attempts at accessing the API inappropriately. The results will be documented on the Automated Monitoring System Review worksheet in the Periodic Ledger. Any issues that are related to potential security breaches will be reported immediately to the Privacy Officer. The review process is as follows:
   1. Fail logging in to the AWS account and ensure the SMS message is sent.
   2. Succeed logging in to the AWS account and ensure the SMS message is sent.
   3. Ensure the AWS config service is running appropriately.
   4. Ensure the fail2ban service is running on each server.
   5. Ensure the nighty scan has been running on each server every day since the last review.
   6. Investigate the number of successful and failed api calls per day since the last review. The server logs will be investigated for days which the ISO determines the number of calls is aberrant.