#### Risk Analysis

##### Scope

This document pertains to the systems that create, transmit, maintain, or transmit ePHI. The complete list of these systems is available on the Criticality Analysis worksheet in the Periodic Ledger tab.

##### System Characterization

Trialomics, Inc systems manage ePHI as follows:

* All ePHI is created by Picard Clients.
* All ePHI is maintained inside an AWS account configured to physically and securely data.
* All ePHI processing occurs either on a Picard Client, an EC2 instance running the Picard API or an AWS elasticsearch instance.
* All transmission of ePHI occurs between Picard Clients and Picard Cloud Environments using TLS/SSL.
* Trialomics, Inc policies explicitly deny remote workforce from storing ePHI outside of servers running in the Picard Cloud Environment.
* AWS manages all physical servers and facilities.

##### Threat and Vulnerability identification

The following list of threat sources has been identified:

* Hackers accessing ePHI through an error in the Picard API
* Hackers accessing ePHI through improper access of the AWS Console
* Hackers accessing ePHI through improper access of AWS Security Tokens
* Hackers accessing ePHI through improper access of EC2 instances
* Hackers accessing ePHI as it is transmitted between security groups inside the Picard Cloud Environment
* Hackers accessing ePHI as it is transmitted between Picard Clients and the Picard Cloud Environment.
* Improper configuration of network security rules

##### Control Analysis

###### Component Hardening

If insecurely configured, operating environments and applications provide opportunities for unauthorized access that could lead to fraud or disclosure of sensitive information. Trialomics has implemented the following “hardening” methodologies to ensure data integrity, security, and availability.

###### Hardening of AWS Account

Trialomics hardens the AWS Account as follows:

* Requires MFA for AWS console access.
* AWS console access is limited to two users.
* Passwords must be at least 10 characters and include one uppercase, one lowercase, one digit, and one special character.
* Passwords should not be used for any other accounts, internal or external to Trialomics.
* IAM access keys are rotated every 90 days.
* Requires SSL/TLS for all external communications via load balancer or ssh port 22.
* AWS CloudTrail is enabled, which provides audit trail capability for the organization to monitor the use of AWS Identity and Access Management (IAM) accounts. An Amazon S3 bucket centrally contains the CloudTrail audit logs. An Amazon CloudWatch alarm or AWS config alerts are configured to send an alert via Amazon SNS: when Root user activity detected, when login attempts fail or succeed, when IAM Configuration changes are detected, when new IAM access keys are created, when security group configuration changes are made, when ssh ports are open to the world, and when changes to the CloudTrail log configuration are detected.

###### Hardening of Databases

The following database hardening features are managed by AWS:

* Removal of unneeded software and operating system components
* Disabling of unused or undesired functionality in software
* Preventing users from installing or disabling software without approval
* Managing encryption and encrypted backups

The following database hardening features are managed by Trialomics through our AWS environment configuration:

* Installation of software-based firewalls limiting inbound and outbound network connections to application servers running the Picard application.
* Removing unused accounts
* Renaming or deleting default accounts
* Replacing default passwords
* S3 storage uses versioning, creating an audit log of all versions and actions carried out on data.

###### Hardening of Servers

Trialomics hardens application servers running Picard applications as follows:

* Removal of unneeded software and operating system components.
* Disabling unused or undesired functionality in software and operating systems.
* Installation of software-based firewalls limiting inbound and outbound network connections. Network connections are limited to subnets in the VPC running the load balancer or database servers.
* Port 22 is closed by default, but can be opened for ssh access through the Amazon Web Console.
* Implementation of access controls on relevant objects to limit system users and programs to the minimum access required.
* Configuration of transfer of local event logs to a central S3 bucket.
* Removing unused accounts.
* Required ssh keys for log in.
* Use of fail2ban on servers to protect against brute force attacks.
* Use of nginx to ban users who attempt to access known vulnerabilities or invalid endpoints.

###### Hardening of Workstations

Trialomics workstations are hardened as follows:

* Installation of antivirus software
* Requiring username and passwords to logon
* Timeouts if not in use for 5 minutes
* Deleting default accounts
* Replacing default passwords

###### Hardening of Picard API

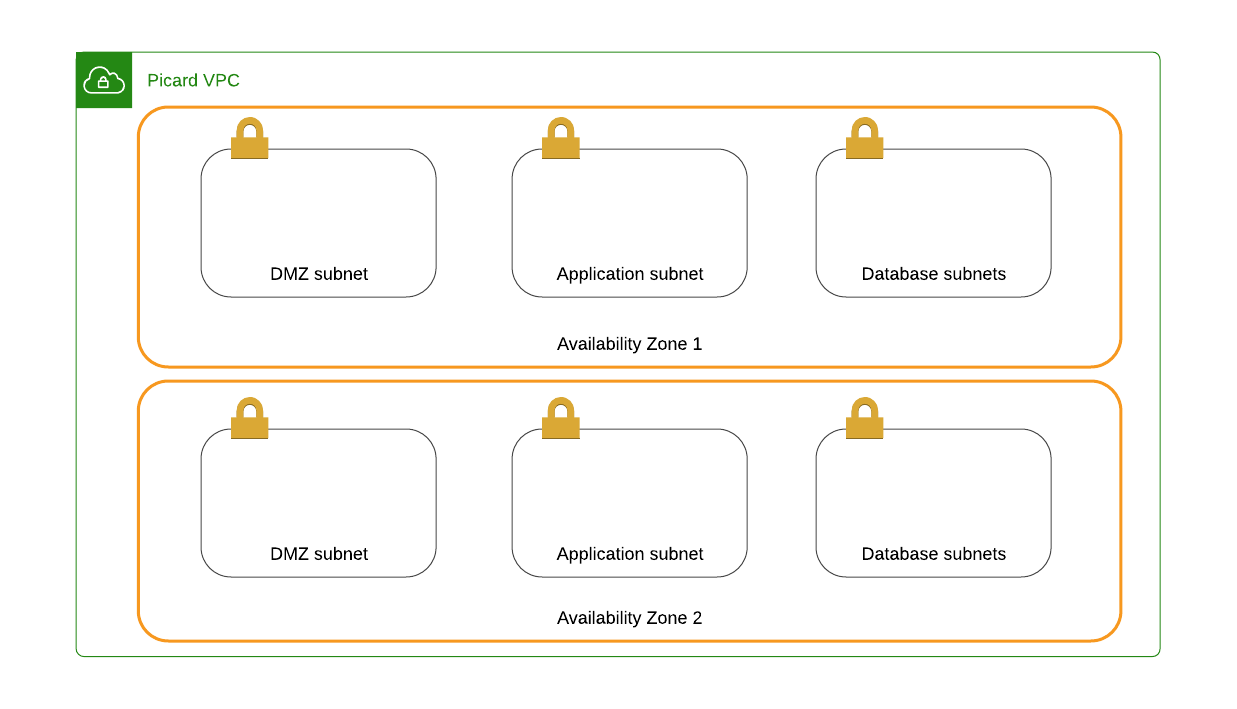
The Picard API is hardened as follows:

* User sessions can be set to expire after a certain period.
* Account creation can require email validation, enabling identity verification.
* Requests can be limited to approved domains, browsers, operating systems, device types, or other features of applications like a security key.
* JSON and Binary Data can be stored and shared using a role based system.
* Failed login requests result in accounts being locked. Unlocking the account requires access to the corresponding account’s email address.
* Users can be forced to provide an SMS token on login.
* Data is stored in three different locations to ensure disaster recovery.
* Administrators have rights to disable user accounts, reset passwords, force password reset through email, create and delete api-keys, and invalidate all sessions.

###### Network Security

Trialomics’ network security is implemented using AWS VPCs, Availability Zones, Subnets, and Security Groups, as well as modifications to application servers. Using security groups and subnets, we ensure the following rules on how critical systems can interact inside a VPC:

* Load balancers require SSL/TLS communications for external communications.
* Within the VPC, load balancers can only pass data to and from EC2 servers running the Picard application.
* EC2 servers can send and retrieve data from load balancers, the RDS, Elasticsearch, and Elasticache databases, as well as S3 buckets.
* RDS, Elasticsearch and Elasticache databases cannot communicate with one another.
* EC2 servers can interact with the Amazon SES and Amazon SNS to send emails and SMS messages, respectively.



###### Redundancy and Backup Plans

Trialomics’ architecture incorporates multiple AWS Availability Zones (AZs) and Amazon S3 storage, which are elemental to organizational plans for the transfer of processing and storage to alternate sites, because this architecture constitutes a built-in alternate storage and processing capability that dynamically provides transfer and resumption of system operations in the event of failures due to fire, vandalism, hardware malfunctions, network/power outages, or a small area natural disaster.

Data storage is limited to the Amazon RDS database, Amazon Elasticsearch database, Amazon S3 buckets, and potentially secondary EBS volumes attached to the application/web server EC2 instances.

AWS built-in features provide a full backup of RDS using a full daily snapshot as well as through transaction logging at approximately five-minute intervals. Other built-in features provide hourly snapshots of Elasticsearch databases. This architecture is configured to retain all backups for the default of 1 day, which can be increased to 35 days by the customer. AWS also employs live storage redundancy for Amazon S3, which provides 99.999999999% durability of objects over a given year. Amazon EBS is replicated across multiple volumes within a single availability zone. Amazon EC2 AMIs are used to store the server environments and configurations across multiple availability zones. Use of these features enables Trialomics to restore any loss of data and quickly resume cloud operations.

Trialomics architecture employs multiple AWS Availability Zones (AZs), which provide alternate storage site capability for data stored in Amazon S3 and Amazon RDS and Elasticsearch databases. S3 uses multiple availability zones by default, and the RDS and Elasticsearch databases deployed within this architecture are configured to be replicated across multiple availability zones, which instantiates a retrievable exact copy of data.

###### Intrusion Detection and Prevention

The ISO will receive a notification when someone fails or succeeds to login to an AWS account. By accessing the AWS account, it is possible to open port 22 through which anyone with a corresponding ssh key can log-in with ssh. SSH keys are kept by the ISO in the KeyPass file, which is stored in location only the ISO and PCO can access. Picard application servers run fail2ban which notifies key personnel on any successful login attempt. After three or more failed login attempts, the user is banned for 60 seconds.

###### Removable Media and Media Destruction

No data is stored on removable drives outside of Amazon Data Centers. Media destruction is managed by AWS. Trialomics returns all data to our customers within 30 days of the contract end date. After the data has been accepted by the customer, Trialomics deletes the AWS account and all data stored within, or deletes the corresponding resources in AWS (S3 buckets, RDS, Elasticsearch, Redis, EC2-servers, Cloudwatch logs).

###### Email Infrastructure

Email provides opportunities for the execution of malicious code, dissemination of content contrary to the Trialomics email policy or of sensitive information to unauthorised users, or attempts to obtain user credentials. Trialomics uses Gmail for its email management. Accessing Gmail accounts of designated staff requires two-factor authentication. The Trialomics policy is to never send ePHI via email.

###### More on API, web applications, and web application security

Web applications provide potential entry points into Trialomics, Inc’s systems if appropriate security measures are not put in place. Custom web applications developed by Trialomics rely on the build console application available only to approved workforce. These applications have the following capabilities:

* Two-factor authentication requiring token sent via SMS for login.
* Session timeout if user inactive for a predetermined period.
* Role based routing to manage which apps are available to which users.

Here is a quick summary of how Trialomics’ platform as a codebase and our internal processes around deploying and hosting stacks address common security concerns.

1. Dependency Injection
   1. All HTTP methods require parameterization:
      * GET and DELETE use query string params which are inputting using the param 'p' which should contain the json request.
      * POST and PUT requests send their parameters using the payload body of the request.
   2. All endpoints enforce parameter type checking.
2. Broken Auth / Session Management
   1. Server side session tokens are hashed.
   2. Account username credentials must be unique.
   3. Session tokens are not included in URLs as parameters.
   4. Login creates new and invalidates any existing sessions, disabling session fixation attacks.
   5. Server side session tokens autoexpire and are invalidated on logout.
   6. SSL/TLS used for all communications, including those involving user credentials and session tokens.
3. Cross-Site Scripting
   1. All pages and components in the Picard Web Console are loaded from an approved \*.picard.io domain. Developers can introduce XSS vulnerabilities through Picard Web Apps, but the responsibility for ensuring this does not occur lies with Trialomics’ customers.
4. Insecure Direct Object References
   1. Each API request includes an access control check to ensure the user is authorized for the requested endpoint and corresponding resource.
5. Security Misconfiguration
   1. Automated scripts are deployed, which removes potential user error.
   2. Build processes are continuously updated to address issues with external dependencies.
   3. State-of-the-art application architecture provides effective, secure separation between components.
6. Sensitive Data Exposure
   1. Authentication via passwords is disabled on all machines. This restricts SSH access to servers to public key authentication only. That is, the only way to log in to your server (aside from the console) is to possess the private key that pairs with the public key that was installed.
   2. User passwords are not stored in clear text, including in backups.
   3. If required, all data stored is encrypted.
   4. All communications with an external client and Picard occur using https. Internally different systems can be configured to encrypt communications, but this is likely unnecessary given the cloud hosting environments in which Picard runs.
   5. All cryptographic algorithms are based on current best practices.
   6. The Picard Web Console and Picard Web Apps do not modify any browser security directives or headers.
   7. The default configuration of a Picard instance does not store sensitive data unnecessarily.
   8. Cryptographic algorithms are FIPS-140 compliant.
   9. Passwords are stored with the PBKDF2 algorithm.
   10. Autocomplete is not used on forms collecting sensitive data and pages in the Picard Web Console are not cached.
7. Missing Function Level Access Control
   1. Picard’s authorization subsystem is a consistent and easy to analyze authorization module that is invoked from all of a customer’s business functions.
   2. All endpoints enforce a permissions check that limits access based on the system roles of the calling user.
8. Cross-Site Request Forgery (CSRF)
   1. On each call, the source origin (from either the Origin or Referer http header) and target origin are required to match. The default origin setting is equal to a Picard domain, others can be added as necessary.
   2. We require a custom http request header, X-Picard: X-Picard, on each request. The heading value can be set to any value.
   3. We respond with a 403 error message for any endpoint request that is not part of Picards API (e.g. phpAdmin/admin).
9. Using Components with Known Vulnerabilities
   1. The security of dependencies are constantly monitored in public databases, project mailing lists, and security mailing lists.
10. Unvalidated Redirects and Forwards
    1. The Picard Web Console limits Redirects and forwards to trusted websites.
    2. URL parameters are never used to calculate the destination.
    3. Destination parameters are always a mapping value, rather than the actual URL or portion of the URL.

###### Software Application Development

Any change to the Picard software must pass a predetermined set of tests in order to be pushed to production and made available to customers. In total, there are more than 1,000 individual tests, each assessing key features of managing users, data, and app configurations The Information Security Officer determines when the software has passed the tests at which point the changes can be pushed to the production servers.

##### Risk Assessment Results

The table below provides an assessment of risks associated with the product and strategies taken or to be taken that mitigate these risks.

| Risk | Magnitude | Detectability | Likelihood | Mitigation Strategy | Course of Action |
| --- | --- | --- | --- | --- | --- |
| Cloud Failure | High | High | Low | Product built into AWS with redundancy at each level. Data is stored across different systems and distinct geographic locations. | Wait for AWS cloud to be restored; depending on which data sources are available, rebuild the environments and applications. |
| EC2 ssh Breach | High | High | Low | Port 22 is closed by default and opening requires access to an MFA token and an ssh key which is stored as an encrypted file and in a location that requires MFA for access permissions. Any login to the AWS account or EC2 server results in an sms or email sent immediately to admins and another email within 24-hours. | The Information Security Officer will receive an email indicating which server has been accessed. If they deem the access inappropriate, they will access AWS Account and stop all EC2 instances attached to the ssh key used for the breach. The exact ssh key name is available via the AWS console for each EC2 instance. |
| Data Center Breach | High | High | Low | AWS will contact Trialomics if there is a breach in their data centers. | Discuss next step with our customers. |
| Database Access | High | High | Low | Accessing databases requires access to the product VPC and security groups. Any such access requires EC2 ssh breach, is logged, and triggers email and text alerts that notify our administrators (See the Mitigation Strategy for EC2 ssh breach for more details). | Similar to what was described for EC2 ssh breach, except that Trialomics shuts down the rds instance. |
| Between Node Connection Sniffing | High | Low | Low | We rely on AWS to secure within VPC communications and restrict inbound access to approved security groups and IAM Roles. | AWS will notify us and we will discuss the next step with our customers. |
| AWS Console Access | High | High | Low | Accessing the AWS account is limited to two individuals. Logins require complex passwords and MFA tokens. | The Information Security Officer receives SMS alerts anytime the AWS console is accessed. If the access is deemed inappropriate, they will contact AWS and ask them to shut down any API requests associated with the account. |
| Network Security Modifications | High | High | Low | Accessing the AWS account is limited to two individuals. Logins require complex passwords and MFA tokens. | The Information Security Officer will receive SMS alerts anytime network security is modified. If the modification is deemed inappropriate, they will log into the AWS account; using the AWS config web portal, ISO will identify which security group(s) has been modified and make the appropriate change. They will then contact AWS and determine how access was gained to understand the full extent of the breach. |
| Inappropriate workstation access when ePHI data in memory. | High | High | Low | Ensure workstations require passwords to wake up from sleep mode. | The Information Security Officer will be notified when a laptop is compromised. They will then notify the Privacy Officer who will make the determination of any need to elevate to the next level. |
| Password Guessing | High | High | Low | If a user fails logging into their account 4 times, the account is locked and they must reset their password via email. Administrators will determine if users will be notified upon successful and/or unsuccessful login attempts. It’s also possible to require an SMS token for logging in, which further reduces the likelihood that an unauthorized user can guess a password while the user is unaware. | It is the customer’s responsibility to notify the Information Security Officer that their account was hacked. The ISO should first ensure the account is disabled before determining what data has been compromised. |

#### 