

## **Trialomics, Inc**

6310 12th Ave NE  
Seattle, WA 98115  
(206) 384-6212

# **Sana Clinical Trial Documentation**

**5<sup>th</sup> January 2020**

## **OVERVIEW**

This document provides a description and a summary of the overall strategy for the validation of the product used by Sana, Inc for their clinical trials.

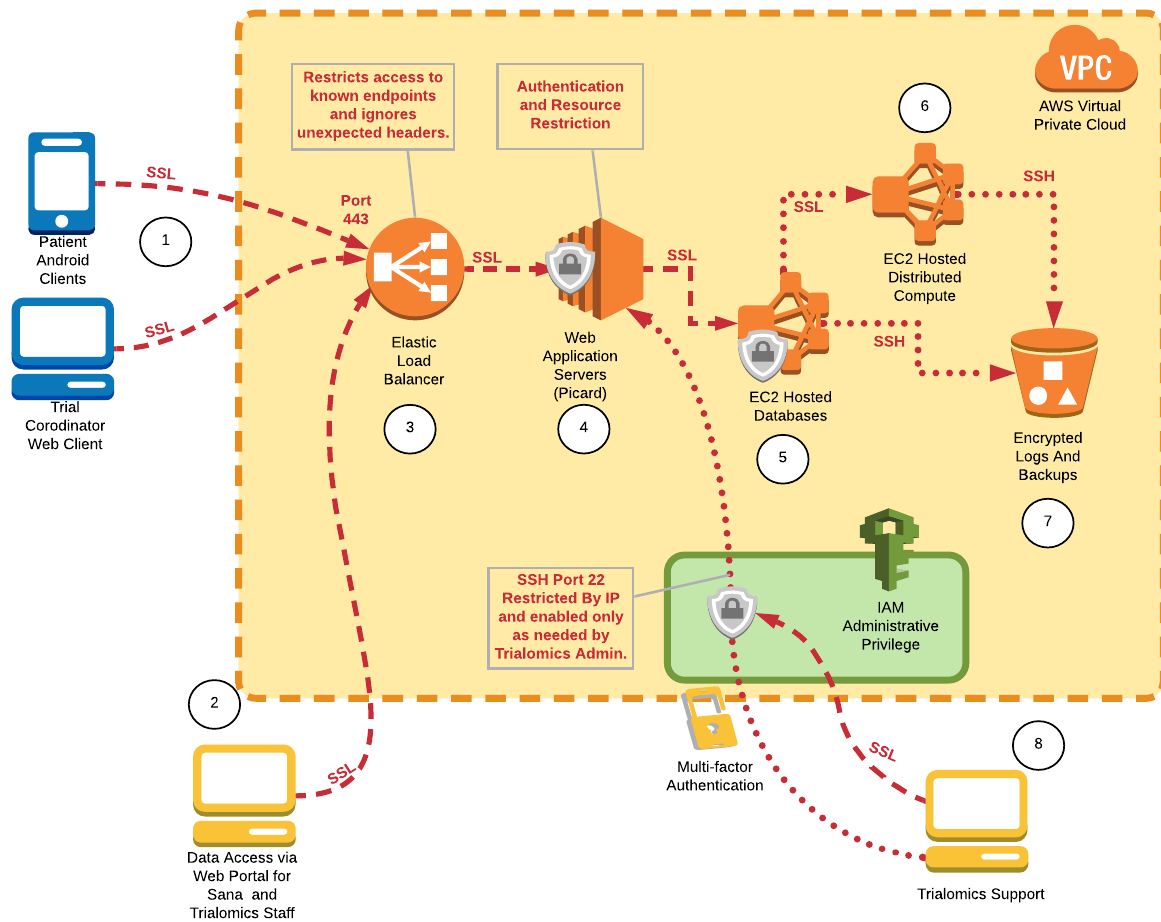
## **SCOPE**

This document is limited to the cloud based environment that runs the web portals and android application used for the trial.

## **PRODUCT DIAGRAM**

### **Cloud Environment**

The diagram below describes the key features of the product.



## RESPONSIBILITIES

All responsibilities for the product testing are assumed by Trialomics, Inc. All responsibilities for testing products developed for the trial are assumed by Sana, Inc. This includes the android app and web portal.

## VALIDATION MASTER PLAN

The purpose of the validation plan is to demonstrate that the critical equipment, systems, and processes perform as designed and intended. Specific equipment, systems, and processes to be validated will be determined based on a documented risk assessment.

## Approach

Qualification Protocols

Qualification protocols are designed to specify the criteria, procedure, testing logic, testing steps and outcome.

## Change Control

Changes to these documents after the product has been released will be addressed as needed. Any updates will include a description in the Change Log section.

## Deviations

Deviations that occur during validation shall be documented and investigated as defined in Qualification protocols. Corrective actions taken or corrective action plans shall be reviewed and approved prior to, or concurrent with, approval of the validation report.

## Documentation

The documentation required for each activity will be defined within the protocol steps for that activity. All observations and results shall be documented in a manner that allows for objective determination of pass/fail status. All protocols shall define the expected results and acceptance criteria. Protocol deviations shall be annotated in the protocol.

## Acceptance Criteria

Qualification protocols define the specific acceptance criteria that must be met to demonstrate that the equipment or system was properly designed, installed, and operated.

## Schedule

Qualification protocols and their corresponding testing plans will be executed prior to the trial. Any changes to hosting environment or flask app will result in testing plans being reexecuted as needed.

## Periodic Review

The document will be reviewed in response to changes in key regulations, customer needs, or relevant events occurring during the trial.

## RISK ASSESSMENT

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

Risk	Criticality	Detectability	Probability	Mitigation Strategy
Cloud Failure	High	High	Low	Product built into AWS with redundancy at each level.
EC2 ssh breach	High	High	Low	Port 22 closed by default; ssh requires key that is stored as an encrypted file and in a location that requires MFA for access permissions. Any login results in an email being sent immediately to admins and another email within 24-hour period.
Datacenter breach	High	High	Low	AWS will contact us if there is a breach in their data centers.
Database Access	High	High	Low	Accessing databases requires access to the product VPC and security groups. Any such access requires EC2 ssh breach and is logged and triggers email and text alerts that notify our administrators.
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.

## FUNCTIONAL REQUIREMENTS AND DESIGN SPECIFICATION

### Controls for Closed Systems (21 CFR 11 B Sec. 11.10)

There are five technical requirements for systems in order to be compliant with 21 CFR Part 11 guidelines for closed systems. The product will meet or exceed all five of these requirements.

#### Accurate Record Generation and Review

The product has the ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by regulatory agencies.

The functionality meets the following requirements of 21 CFR 11:

11.10.b The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.h

The product meets the following requirements:

- 1. Users are able to specify custom search queries and export data in JSON format.**  
Users are able to select search queries, customize queries and view resulting data in JSON format which can be loaded into other software for reporting and analysis.
- 2. Users are able to view patient records and reports through a web portal.**  
Users are able to view records and reports for individual patients or aggregations of patients.

## Program Time-Outs

The program will automatically time-out after 60 minutes of non-activity. The functionality meets the following requirements of 21 CFR 11:

11.10.d Limiting system access to authorized individuals.

11.300.d Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.

The product meets the following requirements:

- 1. Gaining access to the system requires a valid username and password combination.**  
Users cannot gain access without valid credentials.
- 2. The program provides users with the ability to secure the program with logging out.**  
A lack of user activity for 60 minutes invalidates their session and force logs them out of their application.
- 3. The program enforced user sessions cannot be restarted without logging in.**  
User cannot re-enter session without relogging in.

## Audit Trails

The product provides an audit trail, recording all changes to all data. The functionality meets the following requirements of 21 CFR 11:

11.10.e Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.

11.10.k.2 Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

The audit trail is tested programmatically and meets the following requirements:

**1. Computer Generated**

The product audit trail records are generated from a combination of software tools.

**2. Secure**

The product records are securely stored across multiple different databases and objects.

**3. Data/Time Stamp**

The product records have an accurate Date/Time stamp that corresponds to the moment at which the product processed the record.

**4. Journal Function**

The product audit trail records the Date/Time of operator entries and actions that create, modify and delete electronic records.

**5. Unalterable**

Changes to the audit trail do not obscure previously recorded information.

**6. Retention**

Audit trail records are maintained for as long as the retention of the underlying records. The audit trail cannot not be separated from the records.

**7. Accessibility**

Audit trail records are available for FDA review and copying. The audit trail is available upon request and has a single entry for every API request used to modify records.

## Operational System Checks

The product uses operational system checks to enforce permitted sequencing of steps and events. The functionality meets the following requirements of 21 CFR 11.

11.10.f Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

Operational system checks are carried out to ensure validity, security and authorship of all data. For example, the system does not allow data to be modified after it has been created; the system also restricts which users see which data based on their security credentials.

## Device Checks

The product uses device checks to determine, as appropriate, the validity of source data input or operational instruction. The functionality meets the following requirements of 21 CFR 11.

11.10.h Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

Data input is performed through the keyboard and is tested throughout validation, including when testing the apps and web portals used to power the trial. All input forms have validation checks on text, numeric, and date inputs to ensure data is inputted correctly.

## Electronic Signature Manifestations (21 CFR 11 B Sec. 11.50, 11.70)

The product has the ability to secure data through electronic signatures. Data secured with an electronic signature cannot be edited or deleted. Application of an electronic signature requires use of the user's ID and password.

### Electronic Signature and Meaning

Electronic signatures include the printed name of the signer, the date/time the signature was added, and the meaning of the electronic signature. The functionality meets the following requirements of 21 CFR 11:

11.50.a Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

- (1) The printed name of the signer;
- (2) The date and time when the signature was executed; and
- (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

The electronic signature will meet the following requirements:

- 1. Application of an electronic signature requires use of the User ID and password and includes the user name, record meaning and Date/Time when the signature was applied.**

When submitting electronic records users are presented with a web form that presents their name in a disabled field, the meaning in a disabled field and an empty field for password (the user email was entered previously when starting the session). Without entering the correct password associated with the account, the product will not apply the correct signature. The web application and server apply a Date/Time stamp to ensure synchronicity and auditability.

- 2. Data secured with an electronic signature cannot be edited or deleted.**

Once the electronic signature is applied, data cannot be edited or altered.

- 3. Multiple electronic signatures cannot be applied.**

Only a single electronic signature can be applied to each record.

- 4. Electronic record is human readable.**

The electronic signatures are text and human readable.

## Electronic Signature Compliance

Electronic Signatures meet all requirements for 21 CFR 11, including audit trails and password controls. The functionality meets the following requirements for 21 CFR 11:

11.50.b The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).

11.100a Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

## Electronic Signature/Record Linking

Electronic signatures are linked to the respective electronic records in such a manner that the record and the electronic signature cannot be separated, copied, transformed or otherwise falsified. The functionality meets the following requirements for 21 CFR 11:

11.70 Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that signatures cannot be excised, copied or otherwise transferred to falsify an electronic record by ordinary means.

## Electronic Signature Usage

Electronic signatures are used in such a manner that the user must provide consistent, valid credentials and meanings. The functionality meets the following requirements for 21 CFR 11:

11.200.a Electronic signatures that are not based upon biometrics shall:

11.200.a.1 Employ at least two distinct identification components such as an identification code and password.

11.200.a.1.i When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.

11.200.a.1.ii When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

11.200.a.2 Be used only by their genuine owners; and

11.200.a.3 Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

## User Password Controls

The product allows users to update their passwords. It also provides Administrators the right to control user access and security group (Role) membership, define password complexity and time limits, add new users and reset passwords of existing users. The functionality meets the following requirements for 21 CFR 11:

11.10.d Limiting system access to authorized individuals.

11.10.g Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.

11.300.a Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

11.300.c Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.

11.300.b Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

11.300.d Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.

Passwords meet the following technical requirements:

### 1. Limited Access and Unauthorized Access

The product limits access to authorized individuals. User passwords prevent unauthorized access to the system. The product cannot be accessed without an active user email and password. The product enables the deactivation of an account and reports in an immediate and urgent manner any attempts at unauthorized access to the system. This includes notification to the Administrators. The functionality is controlled by the product software.

## 2. Authority Checks

The product uses authority checks to ensure that only authorized users can use the system, electronically sign records, etc.

## 3. Password Uniqueness

The product ensures the uniqueness of each user id, ensuring no two individuals have the same combination of identification code (email) and password.

## 4. Password Periodic Review and Expiration

User passwords expire after 30 days and must be reset before any access is permitted. If a user does not log into the product for 30 days their password expires and must be reset before any access is permitted.

## 5. Password Expiration

User passwords expire after 30 days and must be reset before any access is permitted.

## Additional System Controls

### Event Logging

The product logs every API request, including system log-ins, log-outs, system errors, failed log-ins, record creation and signing, etc.

### System Access

Access to the hosting environment requires MFA access to the AWS account, a decryption key for the encrypted ssh-key, and knowledge of how and which ports to open. Any system access triggers a new alarm sent via SMS message to admins within 5 minutes of activity.

### Input Checks

Where appropriate, entries are programmatically checked by the web portals and apps used to generate the data, as well as by the product to enforce data schemas. This includes combination check boxes and form input validation for text and numeric fields.

## User-Level Security

The table below shows which Roles can carry out which user actions.

Action	Administrator	Trial Coordinator	Patient
Create user accounts	X	X	
Update other users accounts	X		
Delete user accounts			
Create Records	X	X	X

<b>Sign Records</b>	X	X	
<b>Delete Records</b>			
<b>Login to web portal</b>	X	X	
<b>Use android app</b>	X	X	X
<b>Update own password</b>	X	X	
<b>Update other users password</b>	X		
<b>Toggle user account activation</b>	X		
<b>Search data across patients</b>	X	X	

## **Additional Requirements (21 CFR 11 B Sec. 11.50, 11.70)**

### **Procedural Regulatory Requirements**

There are four procedural requirements for systems in order to be compliant with 21 CFR Part 11 guidelines. The system validation tests will ensure the product meets the following requirements:

11.10.a Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

The product documentation covers operating, maintaining, securing, backing up and recovering the services and data. This includes outlining responsibilities for electronic signatures and description of the various encryption and digital encryption standards. The functionality meets the following requirements of CFR 21 Part 11:

11.10.j The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.

11.10.k.1 Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.

11.30 Document encryption and the use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

All personnel using the product will be adequately trained. The functionality meets the following requirement of 21 CFR 11:

11.10.i Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

All data and environments are encrypted and archived in a recoverable, secure manner. The functionality meets the following requirement of 21 CFR 11:

11.10.c Protection of records to enable their accurate and ready retrieval throughout the records retention period.

Changes to the product will be made and tested in a controlled development environment. Any required changes to this document will be made accordingly. All product components, including EC2-environments, software, hosting configuration, and documentation, undergo version control.

## Product Availability and Backup Requirements

The product is available 24-hours per day from anywhere in the world that can access the <https://sana-mshs.picard.io> domain. The data will be backed up daily in an encrypted, secure storage area. Redundancy is built in where appropriate to maximize up-time and availability.

## Testing and Qualification Protocols

Here we demonstrate that the product meets requirements previously established in the Functional Requirements and Design Specification section. Tests are logically grouped and presented in Qualification Protocols. In each protocol we provide the general testing requirements and strategy, and a link to the actual testing documents.

Here is a list of protocols with a summary for each:

## Hosting Configuration, Security and Encryption

The purpose of this protocol is to ensure the Hosting Environment is configured per the product requirements. The tests are executed via a combination of automation and manual inspection of the AWS environments used to create the AML. The key requirements being tested here relate to the following:

- Security and Encryption
- Backups and Disaster Recover
- Fault Tolerance

- Application Support

## API Request Logging and Handling

The purpose of this protocol is to ensure the API requests are logged and handled per the product requirements. The tests are executed via a combination of automation and manual inspection of the AWS environments used to manage API requests. The key requirements being tested here relate to the following:

- Audit Trails
- API request headers
- API Request Flow
- API Request Logging

## EC2 Configuration

The purpose of this protocol is to ensure the EC2 servers are configured per the product requirements. The tests are executed via inspection of the EC2 instance used to create the AMI. The key requirements being tested here relate to the following:

- AMI
- AUTO SCALING
- NGINX
- POSTFIX
- FLASK APP
- CELERY
- CRON
- FAIL2BAN

## Flask App

The purpose of this protocol is to ensure the Flask App meets the product requirements. The tests are executed via a python script. Note we run more than 1,000 distinct tests, but only include relevant tests in the protocol. The key requirements being tested here relate to the following:

- Signing Electronic Records with Audit Trail
- User Accounts, Passwords and Sessions
- Roles, endpoints and data permissions

## **CHANGE LOG**

1-5-2020 Initial release