trackmy

# TrackMy Solutions
# Security Questionnaire

# Contents

# Introduction

TrackMy Solutions is a technology provider focused on making discrete medical record data accessible and actionable to improve overall patient health. TrackMy provides Software-as-a-Service (SaaS) solutions in the state and local government, education, hospital and Ambulatory Surgical Center (ASC) markets, vaccine administration and testing, vaccine verification, general vaccination tracking, primary/secondary education, and occupational/employer health, registration and scheduling spaces. Our vision is to streamline health data access.

We work with industry leading technology partners to bring best in class solutions to the market and help solve some of the healthcare industries most difficult challenges such as data equality, allowing patient's direct access to their data, and providing transparency throughout a patient health journey. We centralize these concepts into a "patient-first" approach which puts the patient in the center of their personal health journey and provides them the tools to be able to manage their own healthcare situations.

# TrackMy Solutions Vendor Information

| | |
|---|---|
| **Company Name** | TrackMy Solutions, Inc. |
| **Product Names** | TrackMy Implants<br>TrackMy Vaccines<br>TrackMy Lab Results<br>TrackMy Verivax |
| **Contact Info** | TrackMy Solutions Security and Technology Officer<br>Contact Name and Title: Kyle Peterman – Chief Information Officer<br>Contact Email: kyle.peterman@trackmysolutions.us |
| **Office Location** | Corporate Office<br>8700 Monrovia<br>Suite 301<br>Lenexa, KS 66215 |

# Employee Information

TrackMy currently employs over 15 employee and contractors worldwide. Every employee has background checks performed prior to employment with TrackMy Solutions, LLC. All full-time employees and contractors have termination policies included in employment contracts that contain a non-disclosure agreement that extends past the termination date.

All associates are trained annually at a minimum on the following policies and procedures:

- Health Insurance Portability and Accountability Act (HIPAA)
- Human Resources Practices (employee handbook)
- Security Awareness Training
- Data Classification and Handling

# Systems Security

## Operating Systems

- TrackMy is a cloud-based software-as-a-service platform, fully hosted in Amazon Web Services (AWS) and delivered over HTTPS.

## Website Encryption Certificate

- TrackMy applications and services communicate via HTTPS, using TLS 1.3

## Hardware/Servers

- TrackMy exclusively uses Amazon Web Services (AWS) Cloud based servers for its architecture.
- Amazon has privacy and information security policies and procedures that align with security best practices. Details can be found at
    - https://docs.aws.amazon.com/whitepapers/latest/aws-overview/security-and-compliance.html

## Anti-Virus Protection

- Internal Windows machines have windows defender antivirus configuration monitored and managed through AWS.
- Linux machines run McAfee Anti-virus and SafeLock monitored and managed through AWS security model.
- McAfee Anti-virus and Safelock are installed on every end-user laptops used to run TrackMy applications and services.
- All AWS servers are protected with Firewalls and Host IDs

### Internal TrackMy Associate Devices

- All new software requested for use at TrackMy goes through a security review process and requires approval before being added to the authorized list.
- Updates and patches are performed on a monthly schedule
- Anti-Virus – All TrackMy users have anti-virus protection installed with regular updates to the virus detection files on a monthly basis.

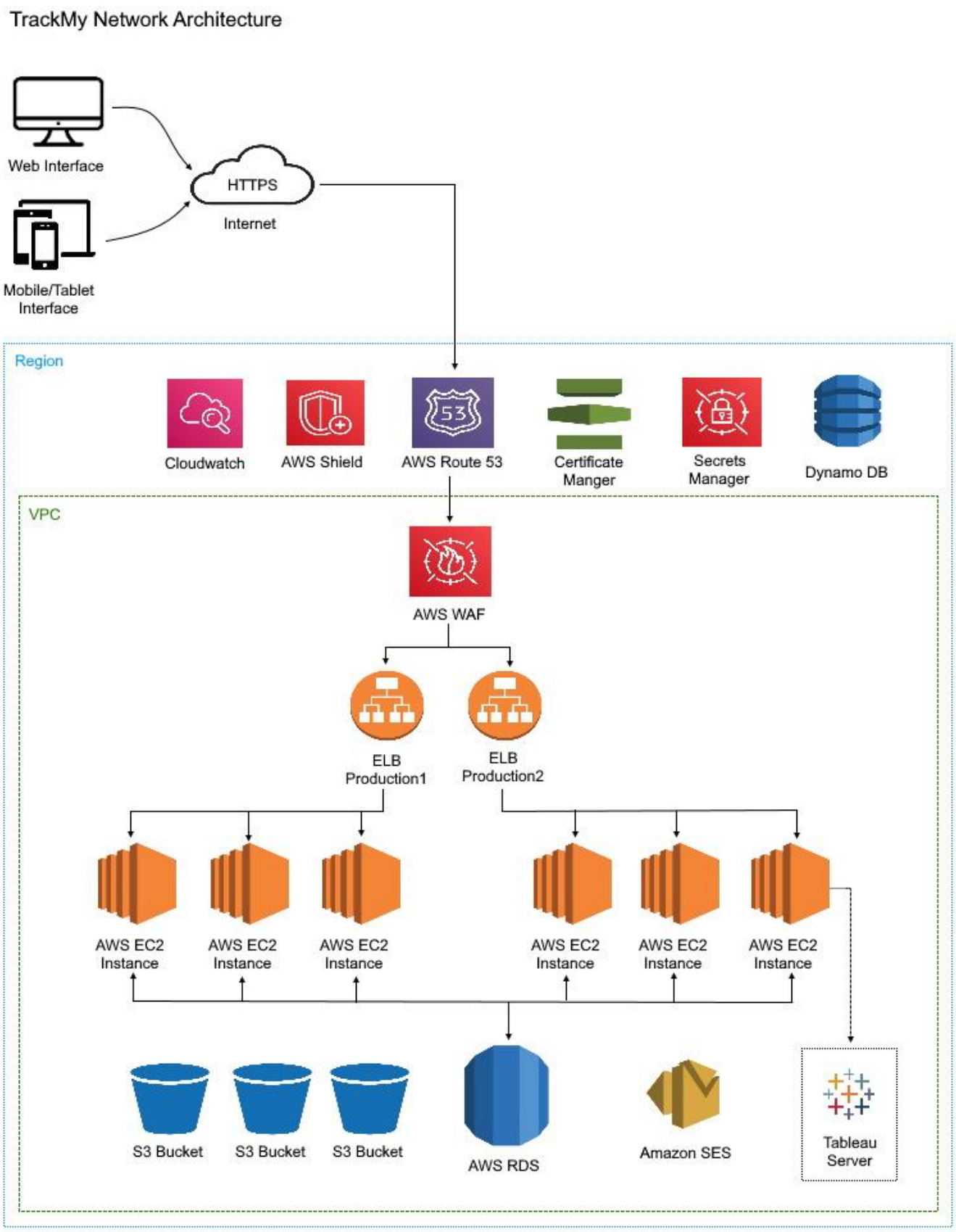
## Cloud Hosting

### Location

- TrackMy exclusively uses AWS Cloud based servers for its architecture.
- All infrastructure components interacting with customer data are hosted within the region of the purchasing customer to comply with regional requirements.
- All production systems are geo-replicated in accordance with customer's regional requirements.

### Third Party Monitoring/Support

- All development, testing and production environments are monitored and supported by our third-party partner Effectual, Inc.  They provide 24 x 7 monitoring and support services for all our environments and AWS services.


TrackMy Network Architecture
Web Interface
Mobile/Tablet Interface
HTTPS
Internet
Region
Cloudwatch
AWS Shield
AWS Route 53
Certificate Manger
Secrets Manager
Dynamo DB
VPC
AWS WAF
ELB Production1
ELB Production2
AWS EC2 Instance
AWS EC2 Instance
AWS EC2 Instance
AWS EC2 Instance
AWS EC2 Instance
AWS EC2 Instance
S3 Bucket
S3 Bucket
S3 Bucket
AWS RDS
Amazon SES
Tableau Server

### High Availability

- Application Servers are hosted behind our AWS Elastic Load Balancers (ELB) with automatic failover in the event that server capacity, scalability or system issues occur. All server instances will failover user sessions automatically.

### Disaster Recovery

- Disaster Recovery tests are performed from backup data restores annually.
- Automated deployment scripts are used for every code deployment, update and patching. These aspects of the disaster recovery plan are tested on a weekly basis.
- Recovery Time Objective (RTO) is 4 hours

### Business Continuity

- Failover will occur automatically when a server is discovered to have issues and no longer able to host client connections. Using AWS Elastic Beanstalk, in cases of a failover, a new server will automatically be spun up and relaunch all applications from the failing server.
- Data recovery/rebuild will occur automatically from our primary RDS to a secondary RDS instance in the event of a primary database corruption or failure.
- TrackMy Solutions has the following cybersecurity insurance policy in place: TrackMy Enterprise Cybersecurity Policy sponsored by The Hartford Insurance Group.

## Risk Mitigation

### Incident Response

- If an urgent incident occurs that requires client interaction, TrackMy staff will contact each of the impacted client's primary contacts via email and/or text/phone call with details of the outage. Short of the loss of multiple AWS data centers, no downtime is expected.
- Expected recovery times and our process will depend on the severity of the incident:
    - Immediately, but not later than 1 calendar day if additional information gathering is required
    - Medium: immediately to 10 calendar days
    - Low grade incidents: immediately, but no later than 30 days
- Security and privacy breach types are defined as: A reportable privacy or confidentiality related event includes any breach in the following requirements:
    - Protected health information is not available or disclosed to unauthorized people
    - Protected health information is not altered or destroyed in an unauthorized manner
        - These are assessed using the HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414.
- Suspected security violations are treated as a reportable event. A nominated administrator at each site is contacted within 48 hours.

## Penetration Testing

- External penetration tests are performed annually by an accredited third-party, covering the TrackMy services and underlying infrastructure.
    - Non-compliances are documented and managed in the normal patching and upgrade schedules
    - No critical issues were found in the prior external penetration test

## Patches

- Effectual, Inc. cloud engineers monitor all server's OS and databases and performs system patch deployments on a monthly basis – 3rd weekend of each month.
- TrackMy maintains N-1 for the OS and database versions.
- Critical/Urgent code patches are performed on a one-off basis if needed before the standard deployment schedule.
- Application releases including new features, improvements, and bug fixes for TrackMy applications are deployed using a weekly deployment schedule.

## Monitoring

- Network Traffic – Network bandwidth and user load is monitored within AWS and adjusted using AWS Elastic Load Balancers (ELB) to throttle the required server capacity up and down.
- Server Load – The CPU and Memory are tracked using AWS CloudWatch to monitor and track CPU and Memory variations.

## System Logs for IT Assets

- Access to TrackMy's information services is limited to TrackMy's corporate network and restricted to approved associates only by Executive Management and Information Security team.
- Access to production databases and systems is restricted to only authorized personnel for specific business use cases. Privileges are reviewed quarterly by the technology executive team and information security team.
- System logs are enabled on all AWS environments and services and stored within a secured S3 bucket within AWS security infrastructure. Logs are kept for 12 months and reviewed annually.

## Change Control

- All attempts will be made to make changes and improvements on TrackMy applications and services without any interruptions to the users.
- Customer Upgrades/Downtime communications will be announced one week prior to the event.
- TrackMy development process follows a standard SDLC process for all new features, enhancement, and bug fixes. This process separates the product owners who define the requirements, developers who enhance and unit test all code modifications, to IT Analysts and QA associates who perform/maintain automated test scripts, feature/enhancement testing and regression testing before new code is released into the production environments.