Clovi

Clovi Platform Security

Whitepaper

Contact us with any questions at
security@clovi.net

Introduction

Clovi is a HIPAA-compliant and HITRUST-ready data management cloud platform for the health screening and coaching industry.

Clovi is committed to following security best practices to protect our customer's data. We strongly believe that the foundation of our business relations is rooted in trust and respect, and a secure data infrastructure is a requirement for such trust and respect to grow.

Clov is trusted by multiple Fortune 500 companies, including Gilead, Cisco, Driscoll's, and Humana. We have successfully undergone external security audits by multiple clients, including SalesForce, world's leading enterprise cloud solution.

The Clovi team consists of world-class engineers and product managers that have secured and scaled cloud platforms in healthcare, finance, politics, and consumer industries. Our team has led engineering efforts at fast-growing companies like Yelp, AltSchool, and NationBuilder, and have worked on web and mobile applications at large institutions like UNICEF, UC Berkeley School of Public Health and UC Davis Comprehensive Cancer Center.

This document outlines Clovi's Cloud Architecture and Compliance Model.

To request more information, contact security@clovi.net

Clovi Cloud Architecture

Division of Responsibility

Clovi products run on Amazon Web Services (AWS) Cloud, world's leading cloud infrastructure provider. By partnering with AWS, Clovi inherits the following infrastructure components:

- Physical and environmental security standards
- Business continuity management processes
- Network security and fault tolerance

AWS physical facilities are secure with active monitoring, total system logging and accredited with ISO 27001, SOC 1/2/3, and other leading physical security measures.

AWS security whitepaper can be found here: AWS Security Whitepaper

Clovi automates its development operations using Aptible, a Docker-based platform provider. By leveraging Aptible's Platform-as-a-Service, Clovi inherits the following security measures:

- 2-factor authentication
- Secure backend access using SSH/SSL
- Automatic, redundant backups
- Firewalls, NAT, Managed VPN and TLS/SSL
- VPC Peering

Clovi web and mobile apps are built by world-class engineers that have secured and scaled some of the world's largest websites. We take care to write secure code and use up-to-date libraries. Within each of our apps, we have secure authentication logic, strict access controls, comprehensive audit logging, and regular security patching.

To request more information, contact security@clovi.net

Visual Reference of Clovi Architecture

All traffic is routed to SSL/TLS endpoint and force HTTPS

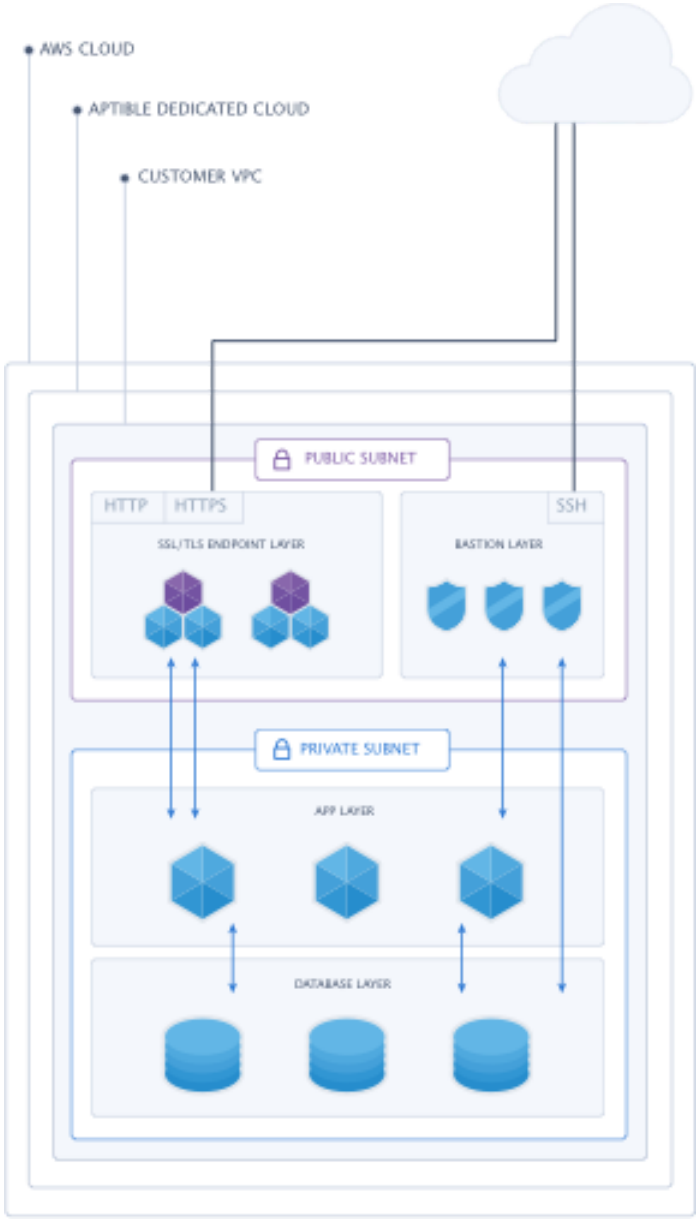
Infrastructure comprises multiple VPN and VPC subsystems.

Apps and databases run in a private subnet, inaccessible from the outside Internet.

Access is restricted to the app and bastion layers.

Database filesystems are backed by SSD and encrypted. Internal database traffic is encrypted.

Encrypted backups are stored in a separate geographic region.



To request more information, contact security@clovi.net

Clovi Compliance Model

Clovi is HIPAA-compliant and HITRUST-ready, and follows a stringent compliance model to manage data security.

Overview

Our Compliance Model consists of 5 parts:

1. Risk Analysis
2. Policies and Procedures
3. Security and Privacy Training
4. Operations
5. Incident Response

Risk Analysis

Clovi has developed a risk model based on potential threats to the health screening and health coaching industry. We regularly update our risk model as new information becomes available, and we constantly monitor and assess security controls.

Policies and Procedures

Administrative controls are designed from the risk model, and meets legal and regulatory (HIPAA, HITRUST) requirements. Regular internal audits ensure requirements are maintained under the administrative controls.

Security and Privacy Training

All Clovi employees and contractors go through rigorous training on how to secure sensitive data. Access to sensitive customer data is limited to specific roles. No single employee has access to ALL the customer data. We have undergone, and passed, multiple external audits.

Operations

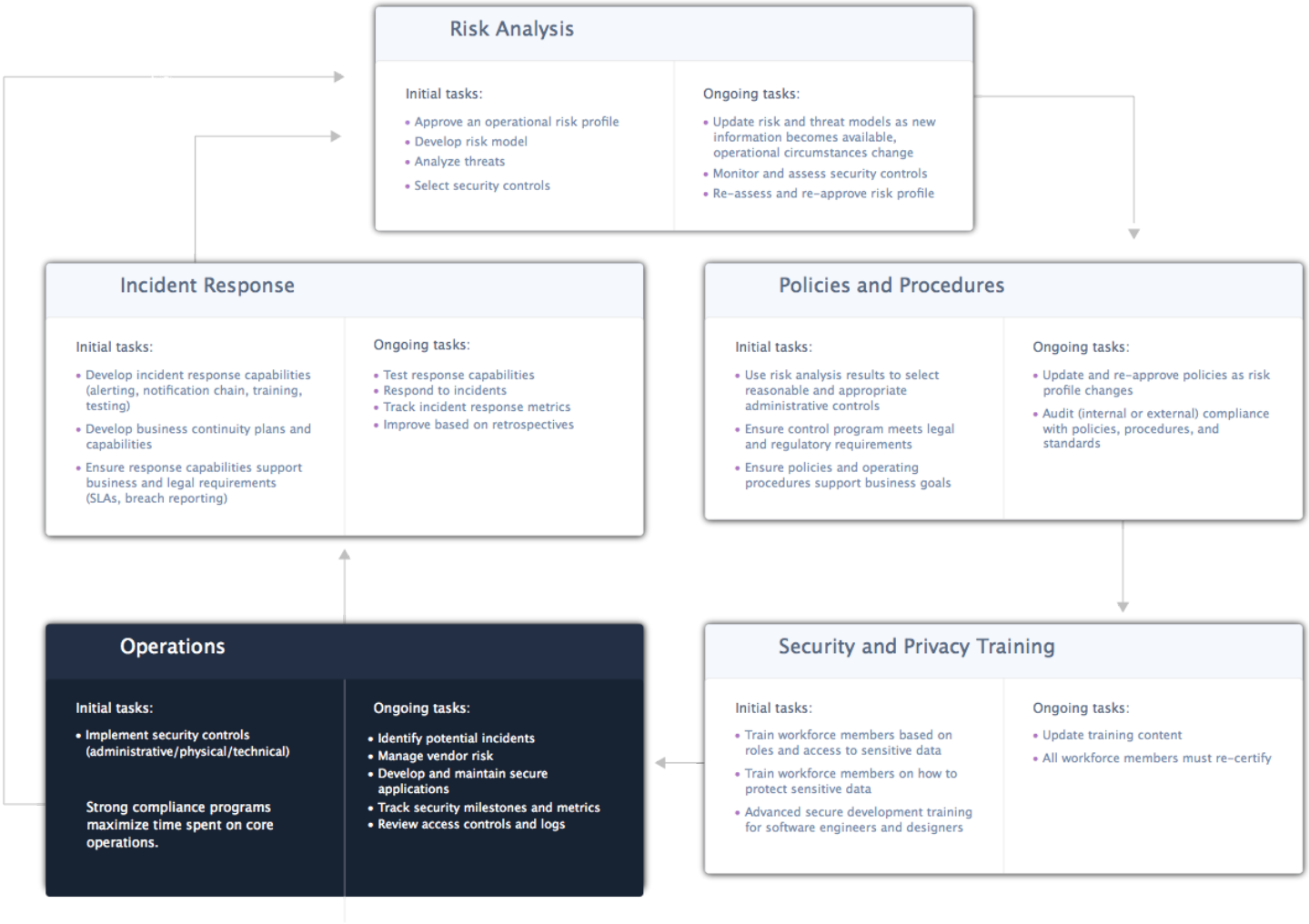
Clovi products are maintained by world-class engineers who have developed and maintained secure applications in the past. We have clear processes in place to review access controls and logs, and to identify potential incidents.

To request more information, contact security@clovi.net

Incident Response

Clovi has developed and tested robust incident response mechanisms, including alerting, breach reporting and notification chains. We maintain and sign agreements with strong SLA guarantee.

Visual reference of Clovi Compliance Model



To request more information, contact security@clovi.net