HEALTHSPARQ®

HEALTHSPARQ SECURITY OVERVIEW

HOW HEALTHSPARQ SECURES AND MANAGES YOUR DATA

LAST UPDATED: JULY 2019

TABLE OF CONTENTS

Note: This document is provided for informational purposes only, and is neither a representation nor warranty of HealthSparq's products or services. It reflects HealthSparq's security practices as of the date of the document, which are subject to change without notice. Any references to third party products or services are for informational purposes only, are not under the influence or control of HealthSparq, and are subject to change without notice. This document does not create any warranties, representations, commitments, conditions or assurances from HealthSparq, or any of our affiliates, suppliers, or licensors. The responsibilities and liabilities of HealthSparq to our customers are controlled by HealthSparq's agreements with our customers, and this document is not part of, nor does it modify, any agreement between HealthSparq and our customers.

HEALTHSPARQ SECURITY OVERVIEW

INTRODUCTION

HealthSparq creates solutions to help people understand and navigate the health care system—and enable them to make smarter health care choices. We partner with health plans so their members can find services, understand out-of-pocket costs and access care. We work hard to ensure the user experience is relevant to each person's unique medical situation, plan benefits and needs.

Health plans and their members trust HealthSparq to responsibly safeguard the data they provide. Maintaining that trust is of utmost importance to HealthSparq and our partners. We are committed to providing a safe, secure and reliable environment for the data entrusted to us. This document provides information about some of the security and reliability resources HealthSparq employs to protect our environments.

COMPANY AND PEOPLE

Security and privacy are core elements of HealthSparq's business. HealthSparq implements physical, technical and administrative security controls to ensure the systems and data under its control are secure. HealthSparq's comprehensive information security and privacy policies and procedures follow industry best practices, and align with relevant regulations, such as HIPAA and HITECH. As a subsidiary of Cambia Health Solutions (Cambia), HealthSparq leverages support and resources of its large parent company. This includes drawing on Cambia's information privacy and security teams in addition to HealthSparq's dedicated teams, as well as routinely engaging Cambia's internal audit division to review HealthSparq's information security policies and procedures.

HealthSparq's commitment to a secure operational environment starts with its people. All HealthSparq employees and contractors are subject to a pre-hire background check, and must complete Security and Privacy Awareness training upon hire and annually thereafter. All workstations use full disk encryption, are configured to prevent the installation of unapproved software, and receive automatic antivirus software updates. New technology is thoroughly assessed and tested by HealthSparq management and Cambia's IT department prior to being authorized for production implementation or deployment across HealthSparq's environment. Only mobile devices managed by HealthSparq can connect to HealthSparq's network.

FACILITIES AND PHYSICAL SECURITY

Access to HealthSparq facilities is strictly controlled. Building entrances are staffed by trained security personnel, and all HealthSparq facility entrances require an RFID badge to gain access. Visitors to HealthSparq are required to sign a security log, and must be accompanied by an escort at all times. HealthSparq's information security policies prohibit the removal of equipment, data or software from HealthSparq facilities without prior authorization.

HealthSparq relies on Amazon Web Services (AWS) for data center infrastructure. AWS data centers are state of the art, and among the most secure cloud computing environments in the world. AWS utilizes many physical security features, including video surveillance, intrusion detection, multi-factor authentication, visitor escorts and trained security staff to control facility access. AWS designs each data center to align with a

variety of IT security standards. More information about the AWS security infrastructure is available at the AWS Data Center Controls page.

RISK AND COMPLIANCE

The early identification and remediation of risks is a high priority at HealthSparq. HealthSparq undergoes regular risk assessments as part of Cambia's enterprise wide Internal Audit Program. The scope of the Internal Audit Program includes review of policies, procedures and technical controls, as well as examining organizational due diligence plans and activities related to:

- Identifying, investigating and resolving risks and threats
- Workforce onboarding, ongoing training and transitioning
- Testing business continuity and disaster recovery plans

Also, on an annual basis, HealthSparq and Cambia jointly retain a third-party firm to conduct a comprehensive HIPAA Risk Assessment of each organization. HealthSparq's risk management activities benefit from the resources available to it from Cambia, including having a dedicated privacy officer and data governance function. To better assess and respond to enterprise risks, HealthSparq integrates Cambia's Enterprise Risk Management (ERM) policy into its strategy management functions.

On the occasions HealthSparq needs to rely on a third party for a product or service, HealthSparq has a formal risk assessment program it uses to evaluate all prospective vendors to determine if the vendor can meet HealthSparq's legal, privacy and security requirements. And, any vendor that will use or process Protected Health Information (PHI) with HealthSparq must enter into a Business Associate Agreement (BAA) with HealthSparq.

IDENTITY AND ACCESS MANAGEMENT

Across its workforce, HealthSparq practices role-based access, and grants system access to employees and contractors based on the principle of least privilege. Workforce members, including contractors, are assigned unique user IDs, and HealthSparq prohibits the use of shared logins except to access training, demonstration or other "sandbox" accounts. HealthSparq enforces strict password controls for access to internal systems. Access to information security management systems is limited to employees who require access to perform their job duties, and is monitored using AWS CloudTrail.

HealthSparq user access is provided through federated ID access management, where users are validated by HealthSparq's customers. HealthSparq customers maintain a directory of their authorized users. Our flagship product, HealthSparq One®, is designed to integrate with customer SSO solutions so that when the user logs in to the customer portal, HealthSparq One trusts the customer portal to validate the user as authorized. This allows users to access HealthSparq One without storing their credentials with HealthSparq or requiring customers to enforce HealthSparq's password policies. HealthSparq One connects to customer portals using SAML 2.0.

INFRASTRUCTURE AND AMAZON WEB SERVICES

HealthSparq uses Amazon Web Services (AWS) as its hosting vendor for HealthSparq One. AWS is one of the most secure cloud computing environments in the world, and maintains a robust array of security

certifications[1], including SOC 2, ISO 27001 and FedRAMP. AWS data centers and network architecture meet the needs of the most security-sensitive industries and organizations. AWS data center regions connect to multiple ISPs. HealthSparq leverages a spectrum of services provided by AWS, including Simple Storage Service (S3) and Elastic Load Balancing (ELB), to ensure high availability and redundancy of HealthSparq data. HealthSparq connects with AWS data centers via a number of secured/authenticated connection mechanisms, including:

- HTTPS
- TLS1.2
- AES128
- SSH
- Multi-Factor Authentication (MFA)
- Identity and Access Management (IAM) Keys

HealthSparq uses an infrastructure as code (IaC) approach to securely automate the development, configuration and deployment of immutable environments such as containers and virtual machines. HealthSparq One uses an enterprise-grade web application firewall to filter and secure inbound traffic as a defense against application layer security threats. HealthSparq environments are isolated and continuously monitored, using continuous integration and delivery (CI/CD) defect logging and monitoring.

The HealthSparq network is segmented using AWS EC2 Security Groups (*i.e.*, virtual firewalls), Virtual Private Clouds (VPCs) and subnets to segregate the DMZ (demilitarized zone) from the rest of the network, and to segregate sensitive data stores from the rest of the environment. HealthSparq processes, stores and transmits PHI using only HIPAA compliant services which are configured to AWS requirements in accordance with HealthSparq's business agreement with AWS.

CODING/DEVELOPMENT AND CHANGE CONTROL

To ensure a secure product environment for its customers, HealthSparq implements industry best practices in the operation of its HealthSparq One platform. HealthSparq develops its products following secure Software Development Lifecycle (SDLC) practices in accordance with Open Web Application Security Project (OWASP) coding guidelines, employing a combination of manual and automated review processes. Production and non-production environments are logically separated.

HealthSparq's technical ecosystem is an automated code pipeline that supports the development of integrated applications, such as HealthSparq One. HealthSparq developers follow behavior-driven development (using Cucumber) and testing methods, allowing for automated code development. HealthSparq's development ecosystem enables developers to use automated processes to easily and securely replicate microservices across multiple applications. Automated development and testing processes include scanning code for vulnerabilities prior to each production release, and testing code for integrity, data leaks and complexity.

HealthSparq implements immutable infrastructure and services for significant security and change management benefits. Immutability ensures that services and infrastructure cannot be modified post-deployment. Unlike traditional infrastructure components that expose administrative ports and allow

[1] A comprehensive collection of whitepapers describing security and compliance at Amazon Web Services is available at https://aws.amazon.com/whitepapers/#security.

modifications in place, changes to HealthSparq services and hosts can only be performed via retest and redeployment.

HealthSparq One code undergoes defect scanning in its delivery pipeline. Post-production, HealthSparq continues to scan code for vulnerabilities. HealthSparq's manual processes include peer review for every feature unit, and reviewing all shared code at the beginning of each sprint. HealthSparq follows an established vulnerability management program that includes the following:

- Annual third-party penetration testing and system audits
- Regularly planned maintenance periods
- A documented patch management process

Changes to HealthSparq's systems are made in accordance with HealthSparq's formal change management process. The use of new applications, systems, databases, infrastructure and services within HealthSparq must be approved by HealthSparq management and Cambia's IT department prior to being made available to users. HealthSparq reverts to the previous configuration in the event a planned change is unsuccessful. In the event circumstances do not allow for the formal change management process to be followed, HealthSparq has established emergency procedures to manage necessary changes. Required steps in HealthSparq's change management process include:

- Forming the change-plan, which must include a defined back-out process
- Authorization to commence development of the planned change
- Extensive testing of the change, including user acceptance testing
- Security review of the change
- Formal approval to deploy the change into production

DATA SECURITY/DATA LOSS PREVENTION

HealthSparq understands the importance of protecting its customers' data. Data transmitted to HealthSparq One is fully encrypted both in transit and at rest. Within HealthSparq One, customer data is abstracted and stored using logical segmentation, and is never commingled with other customers' data. The HealthSparq One application is encrypted, and transmits PHI within AWS environments using TLS 1.2 256-bit encryption. User passwords are never stored by HealthSparq because HealthSparq One is specifically designed to integrate with customer SSO solutions. Customer data is neither stored nor transmitted outside of the United States. HealthSparq uses a third-party data loss prevention (DLP) solution that is configured to identify the presence and prevent dissemination of sensitive information in email, uploads and files copied to removable media.

LOGGING AND MONITORING

HealthSparq utilizes a variety of commercial security incident logging and monitoring tools to monitor access and changes to HealthSparq systems. Access to HealthSparq systems is monitored 24/7 by Logging and Event Management (LEM) tools. Event logs are aggregated and monitored continuously by a Security Incident Event Management (SIEM) system. HealthSparq One uses AWS Shield to monitor incoming traffic and automatically mitigate Distributed Denial of Service (DDoS) attacks. An automated platform continuously monitors the security and compliance of HealthSparq's cloud configurations against internal baselines. Each of these services notify HealthSparq's information security team of potential security incidents.

INCIDENT RESPONSE

Cyber security incidents are an increasingly frequent reality of today's computing climate, so it is imperative that service providers be prepared to respond. HealthSparq's preparation begins with maintaining a documented incident response process that is reviewed and updated annually, and more frequently as needed. The process includes mitigation strategies and communication procedures.

HealthSparq's response process starts with being able to rapidly detect suspected security incidents and isolate any affected systems. The commercial monitoring tools HealthSparq deploys across its environments push real time notifications to HealthSparq's information security team when potential security incidents are detected. Suspected incidents are evaluated and categorized based on severity. The information security team is trained to follow chain-of-custody procedures, including creation of a forensic image of the affected system(s) at the containment stage when appropriate. Following containment, HealthSparq's information security team determines if the suspected incident was a security event, or another type of incident, and promptly notifies the appropriate internal resources. HealthSparq and Cambia select which enterprise incident response process to follow based on the incident or event type determined by the information security team. After any incidents are eradicated in accordance with the appropriate process, recovery procedures are run on the affected system(s).

AVAILABILITY AND DISASTER RECOVERY

AWS is renowned for providing reliable environments with a high resiliency to outages. HealthSparq ensures high availability and fault tolerance from its production environments by distributing active workloads across separate availability zones in the same region. Each AWS region is connected to multiple ISPs. HealthSparq utilizes AWS services (such as S3 and Elastic Load Balancing) that are designed to provide high availability and redundancy. Critical areas of HealthSparq's architecture are designed as redundant clusters, including the following: anti-bot/scraping servers, web load balancers, web servers, application load balancers and application servers. When compute resources reach a predefined utilization threshold, additional compute resources are immediately added via provisioning scripts—allowing the system to scale horizontally and vertically. To further mitigate against the risk of a disaster or other event affecting data centers, HealthSparq's AWS production data center is located in a geographically-distant region from its AWS recovery data center.

HealthSparq leverages AWS IaaS features to host its production data center. HealthSparq's production data center transmits back up data over an encrypted link to its disaster recovery data center. At its recovery data center, HealthSparq uses AWS Cloud Protection Manager to back up instances and Elastic Block Store volumes. In addition, redundant storage across multiple physical facilities is a normal operation of many AWS data storage services.