Castlight

Castlight Health's Approach to Security

January 2021

Table of Contents

Introduction

Castlight Health, Inc. (herein referred to as “Castlight” or “the Company”) is on a mission to make it as easy as humanly possible for individuals to navigate the healthcare system and live happier, healthier, more productive lives.

Our health navigation platform connects hundreds of health vendors, benefits resources, and plan designs into one comprehensive health and wellbeing experience.

Castlight transforms employee benefits into a deeply personalized, simple, and guided experience, empowering better-informed patient decisions to unlock better healthcare outcomes and maximizing return on healthcare investments.

Castlight delivers this offering to registered customers through our website and mobile application downloadable from the App Store and Google Play Store.

This guide is designed to provide interested parties with an understanding of our approach to security highlighting the practices, activities, and commitments we maintain to safeguard your data.

Data Overview

In order for interested parties to evaluate our approach to security and the risks associated, it is important to understand what types of data are involved. As a health navigation platform, our customers provide us with a limited set of data, which may be considered Sensitive Personal Information, about their employees and dependents. This data is used to verify the eligibility of the individuals for Castlight services. To provide our services, we receive data from the individuals during their registration process and throughout their subsequent participation. The data provided may contain Protected Health Information, and it is our responsibility to safeguard the data in accordance with our Terms of Use and the HIPAA Privacy Rule.

As such, Castlight has established a framework for classifying and handling data received or created by Castlight. Our classification framework is designed to align with the information security objectives of confidentiality, integrity, and availability.

Public Data

Castlight classifies Public Data as information that is authorized for distribution to a public audience. Such data may be broadly distributed without negative impact to Castlight, its employees, stakeholders or customers.

Internal Data

Castlight classifies Internal Data as proprietary company information related to the Company's internal operations that is not public. Internal Data also includes company confidential information related to the management of secure communication and transmission of protected data.

Unauthorized disclosure of Internal Data, particularly outside of the Castlight, is likely to cause damage to the organization, its employees, stakeholders or customers.

Restricted/Confidential Data

Castlight classifies Restricted/Confidential data as non-public personal information. Restricted/Confidential Data is information received from our customers or end users and processed by Castlight to provide our services.

Restricted/Confidential Data is information that if lost, compromised or disclosed, could result in substantial harm to the Company, its stakeholders, customers or end users. As such, Castlight strictly restricts access to this classification of data to authorized company personnel based on their job responsibility. This classification of data is separated into subclassifications as detailed below.

Personal Information

Personal Information (PI) is general non-public personal information. This type of data includes an individual's name, address, phone number or email address.

PI also encompasses Sensitive Personal Information (SPI) which includes health plan eligibility, social security numbers (SSN), certain biometric data and user Protected Health Information (PHI) which is further defined below.

Personally, Identifiable Information

Personally, Identifiable Information (PII) is user information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

Protected Health Information

Protected Health Information (PHI) is information in the medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service such as diagnosis or treatment.

Castlight’s Security Culture

Castlight believes everyone plays a critical role in keeping our data secure. As such, we cultivate an organizational culture that is both aware and proactive about security risks. Our security culture is fostered throughout the Company via training, dedicated personnel and regular communications.

Security Training

Castlight employees and contractors undergo mandatory security training as part of the onboarding process and receive continuous training throughout their Castlight career. During orientation, new employees agree to our Employee Handbook, which highlights our commitment to keep data secure. The security training, which is renewed on a regular basis, includes topics like HIPAA, phishing and privacy regulations. For employees in technical positions, additional training around application security and secure coding practices is provided.

Access to Castlight internal systems is revoked for employees and contractors who are non-compliant with our security training requirement.

Our Dedicated Team

Castlight employs security, compliance and privacy professionals who are tasked with implementing security policies, maintaining our defense systems and developing security review processes for continuous monitoring.

The focus areas of Castlight’s dedicated Security Team include actively scanning for threats using best-in-class tools, monitoring for suspicious activity and performing routine security evaluations and audits. The Security Team also engages in company-wide outreach and communication to cultivate our security-minded culture.

Castlight’s compliance and privacy professionals work alongside the Security Team to further safeguard your data. The Compliance Team is responsible for maintaining compliance with regulations, in addition to determining key systems, processes and related controls supporting independent audits and assessments. Our Privacy Team is responsible for setting privacy best practices, continuously reviewing changes to regulations and standards, and assessing the privacy practices of third-party vendors to ensure Castlight adheres to strong privacy standards.

Awareness within the Organization

Castlight believes that for everyone to embrace our security culture, they must be equipped with the appropriate knowledge and resources. In addition to our formal security program and mandatory security training for all personnel, the Security Team works to continuously promote awareness within the organization.

The Security Team provides the company with important security news updates and relevant resources on a regular basis. The team also publishes blog posts that are available company-wide to provide useful information on a wide range of security topics.

The Security Team communicates general security processes and procedures to all Castlight personnel to promote proactiveness. Security procedures, such as incident reporting, are core knowledge to ensure correct and timely actions are taken to best protect your data.

Shared Security Responsibility Model

Castlight's products are designed and operated with security in mind.

To deliver our service with consistent confidentiality, integrity and availability to every customer, Castlight operates under a shared security responsibility model.

The shared security responsibility model is a framework adopted by service providers to identify the distinct security responsibilities of the customer and the service provider.

Castlight's Responsibility: Security of the Application

Castlight is responsible for the security of the application and its underlying infrastructure. Castlight is also responsible for providing features you can utilize to secure your data in the application.

In the next section, "Castlight Security Controls", we have provided a high-level overview of the controls implemented to protect the security of our infrastructure.

Your Responsibility: Security for the Application

Our customers are responsible for data integrity and access management within the Castlight application. As Castlight will be a benefits platform used by your employees, Castlight relies on our customers to send accurate and consistent data.

Castlight also strongly encourages all customers to enable the multi-factor authentication features offered within Castlight services for your employees. Our combined partnership will help prevent and reduce the risk of incidents.

Castlight

Security Controls

Physical & Infrastructure Security

Castlight maintains a formal and comprehensive security program designed to ensure the confidentiality, integrity and availability of our systems and data while protecting against the threats faced by a modern enterprise.

Principles such as least privilege, strong authentication, irrefutable audit trails and guaranteed data integrity are implemented through controls such as mandatory multi-factor authentication, firewall-enforced network segmentation, encryption in transit, encryption at rest and behavioral-based activity monitoring. These controls are universally enforced across our environment to afford a consistent level of protection. The security program is routinely reviewed in conjunction with our customers, partners and vendors to improve our practices and adjust to the changing threat landscape.

Physical Security

Data Centers

Castlight's primary and secondary data centers are physically maintained by third party service providers. The service providers provide physical security that meets or exceeds industry standards and have achieved, at a minimum, ISO 9000, ISO 27001, PCI-DSS and SSAE18 certifications.

Physical security features include 24/7 on-site personnel, CCTV surveillance system, key card and biometric secured facilities and multiple layers of security. The environmental infrastructure includes chillers and cooling towers, leak detection systems, fire suppression systems and a fire station adjacent to the property. The service providers have an automated monitoring and alerting system on the mechanical, environmental and electrical infrastructures.

Both the primary and secondary data centers are designed to be fully redundant and located in geographically stable locations.

Corporate Offices

Castlight corporate offices are secured and controlled by 24/7 on-site personnel, the use of key cards and an electronic access system. Access is monitored through CCTV surveillance system, and recordings are retained. The corporate offices have defined security perimeters with additional security for equipment rooms. Equipment rooms do not store any critical systems. Corporate offices adhere to local health and safety regulations and OHSA requirements.

Infrastructure Security

Castlight is a multi-tenant Software as a Service (SaaS) application leveraging a service-oriented architecture.

Data Acquisition

Castlight customers will provide a limited set of data, either directly or through their partners, of participants eligible for Castlight’s services. This eligibility file will be sent to our secure server via Secure File Transfer Protocol (SFTP). The file transfer from our customers is encrypted prior to transmission using industry standards at a minimum of Advanced Encryption Standard (AES)-256. Outbound files sent by Castlight are transferred using the same security standards mentioned above.

Data Validation & Integration

Castlight has a strong data validation framework to ensure that the data being ingested into our system is accurate and secure. Once eligibility files have been received via SFTP, our Extract, Transform, Load (ETL) process is triggered to process the file into our data warehouse. The ETL process checks for quality metrics and generates a validation report upon completion. Deviations from these metrics are triaged by the data management team and resolved in a timely manner.

Data Warehouse

Application and customer data are stored on servers owned and centrally managed by Castlight. Physically, the servers are maintained by our service providers. As a multi-tenant application, customer data is logically segmented through the use of unique employer identifiers.

Data-at-rest is encrypted using industry standards at a minimum of AES-256, and data-in-transit is encrypted using industry standards at a minimum of Transport Layer Security (TLS) 1.2. In addition, access to our data warehouse is strictly controlled using the least privilege access policy to ensure access is only granted to authorized personnel. User access is monitored and reviewed regularly.

Patch Management

Castlight has implemented a vulnerability patch management program to minimize the risk of threats and potential vulnerabilities. Vulnerabilities are rated according to risk factors, such as location and impact, to prioritize remediation. The Security Team prioritizes critical vulnerabilities to be actioned on a timely basis based on factors mentioned previously.

Our vulnerability management strategy and program focus on centralizing and automating operations to promote organization alignment to security principles and is an integral part of overall security management.

Web Security

Castlight monitors the current threat landscape to help identify attacks and attackers before they cause damage or disruption to our customers. To meet this objective to protect, detect and respond to advanced threats, we have implemented a suite of tools to help prevent attacks, identify high-risk activity and quickly respond to incidents.

As part of our toolkit, Castlight has implemented web application firewall (WAF) features including Distributed Denial of Service (DDoS) attack protection, origin defense and advanced bot detection. These controls work in concert with our intrusion detection system (IDS) for rapid threat detection and intelligence.

For additional details about our complete suite of security tools, interested parties can request a copy of our SOC 2 Type II report.

Backups

Castlight has a backup policy in place to safeguard application and customer data, prevent the loss of data and provide timely restoration in the event of an unexpected incident.

The servers on which the application and customer data resides are backed up real time to our secondary data center. Backups are encrypted in transit and at rest using industry standards such as TLS 1.2 and AES-256, respectively. As per our retention policy, Castlight retains backups in accordance with its criticality and permanently deletes old ones.

Logging

The protection of data against breaches of confidentiality, failures of integrity or interruptions to its availability to authorized users is essential to our mission. To achieve this, we maintain centralized audit logs of application, data and operating systems to capture key events including connection attempts, file transfers and administrator activities.

Monitoring

Castlight employs automated systems deployed throughout its environment to monitor key events and analyze system logs, the results of which are regularly reviewed. These monitoring systems support near real-time analysis as well as the alerting of events and the integration of intrusion detection into access and flow control mechanisms.

Castlight employs a suite of tools for monitoring and alerting equipped with robust dashboard functionality, along with alerts and notifications providing for intrusion detection and analysis. Automated tools are also used for alerting and monitoring our infrastructure, networks and operating systems for availability and performance issues.

Event Management

Castlight employs a Security Incident Event Management (SIEM) tool to monitor production host, network, and application logs. The SIEM tool generates automated alerts which are monitored with 24/7 coverage. Critical events are escalated and reviewed by the Security Team in a timely manner.

Firewall Change Management

Castlight’s network is logically segmented through the use of internal and external firewalls. By policy, Castlight maintains a default deny policy on our firewalls. Changes made to firewall configuration are reviewed and approved by the Security Team before implementation.

Customer Offboarding

In the event that the relationship between Castlight and a customer ends, customer data will be purged and de-identified from our data warehouse using Safe Harbor guidelines. This is executed within the timeline specified in the customer contract.

Availability, Performance & Continuity

Service Level Agreement

Castlight will provide a 99.9% uptime guarantee.

Maintenance Window

Castlight performs upgrades and maintenance on the application on a continuous basis, normally without impacting availability. Castlight reserves a maintenance window as agreed upon in contracts to perform maintenance that could impact availability.

Availability Monitoring

Castlight maintains automated monitoring and alerting of system availability and performance.

Disaster Recovery

Castlight implements a comprehensive Disaster Recovery Plan (DRP) designed to enable us to meet our existing obligations to our customers in the event of an emergency or significant business disruption. The Disaster Recovery plan specifies RTO and RPO objectives based on service criticality and is tested at least annually.

Business Continuity

Castlight implements a comprehensive Business Continuity Plan (BCP) designed to enable the company to meet existing obligations to our clients and counterparties promptly in the event of an emergency or significant business disruption. The plan is designed to work in many different emergency situations and is tested at least annually.

Incident Response

Castlight has a formal incident response plan established to respond, report, escalate and triage reported security events. The guidelines and procedures are documented to provide a defined, organized approach for handling and resolving any potential threat to systems and data.

Personnel Security

Least Privilege Access Policy

Castlight systems and applications are configured with role-based access using a Least Privilege policy. Logical access controls are in place to clearly define user access profiles and grant access based on need-to-know, need-to-share requirements.

Castlight has established an access authorization process to address requests for access, changes to access, removal of access and emergency access. Access to sensitive environments is restricted by default, and temporary access is granted for emergency use.

Castlight performs user access reviews on a periodic basis to review user accounts and services with access to sensitive data.

Secure Personnel Practices

Before Hiring

Castlight conducts a background investigation of all employees and contractors prior to employment. Castlight outsources our background checks to a service provider, which uses Fraud and Control Information System (FACIS) search.

Upon Hiring

Castlight employees and contractors undergo HIPAA and security training as part of the onboarding process. During onboarding, new employees and contractors agree to our Castlight Health Employee Handbook, which highlights our commitment to keep customer information secure.

While Working at Castlight

Castlight staff (employees and contractors) use unique, dedicated credentials to access Castlight systems. These staff accounts are managed through an identity and access management system.

Multi-Factor Authentication

Access to Castlight’s systems is controlled by a Single Sign On (SSO) solution that enforces Multi Factor Authentication (MFA). These MFA controls are extended to our internal environments as well to control remote access to our environments via a secure virtual private network (VPN). VPN access is restricted to authorized users and requires MFA.

Password Policy

Castlight password policies meet or exceed industry standards, including the latest advisory from NIST 800-63b for all Castlight users.

Laptops and Desktops

Employees are issued a Castlight managed laptop or desktop computer. Devices are configured to only allow the installation of authorized software. Local administrator access is controlled and limited to authorized users only. All users are bound by an Acceptable Use Policy.

Clean Desk Policy

Castlight’s secure workplace guidelines require employees to remove sensitive information from accessible locations at their workstation and secure their desk or office at the end of the day.

Mobile Devices

Castlight allows employees to use personal mobile devices, subject to a bring your own device (BYOD) policy and company approval. Employees using personal devices are required to meet minimum standards, including installing a Mobile Device Management (MDM) solution. Castlight MDM has the ability to remotely lock and wipe devices when lost or stolen.

Digital Loss Prevention

End-user computers have a Digital Loss Prevention (DLP) utility installed that allows Castlight to monitor end-user activities. DLP activity is centrally reported, alerted upon and audited by the security team.

Anti-Virus

End-user computers have an anti-virus utility installed. It is configured to install signature updates automatically upon release. All computers report the status of their anti-virus utility to a central server that is monitored by the Security Team.

Removable Media

End-user computers are configured to block access to removable media such as USB drives.

Authorized Software

Authorized software is reviewed by Corporate IT and pre-loaded into a self-service portal for employees to install.

When Departing

Castlight's offboarding process is initiated by a notification from Human Resources. Castlight staff accounts are disabled on their termination date through the identity and access management service. Both physical and logical access is removed, and company assets are required to be returned in a prompt manner.

Software Development Security

Software Development Life Cycle

Software Architecture

Castlight is a multi-tenant SaaS application with native iOS and Android clients, as well as a responsive web client. Our architecture is designed to allow us to build redundancy and efficient scalability into our application.

Training

Castlight engineers receive security training focused on understanding Castlight's Security Program and preventing security vulnerabilities as identified by commonly accepted industry standards including the OWASP Top 10.

Build and Deploy

Castlight uses an automated build and deploy process to perform scheduled promotions to production. This limits manual interventions and allows for numerous code checks and approvals by relevant parties along the deployment path.

Code Testing

Castlight's build and deploy process includes automated code testing including unit testing, dynamic testing and static analysis. Testing must meet pre-determined thresholds and all outcomes are tracked. Any relevant failures are tracked and worked to resolution by a devoted Quality Assurance (QA) team and code development teams.

Environments

Castlight maintains multiple separate development and production environments that are logically separated. The development environment is a replica of the production environment with non-sensitive data.

Release

Castlight maintains a defined release cadence and approvals must be documented prior to all release activities. All release plans require detailed roll back plans. During deployment, Castlight's Quality Assurance teams work in real time to validate that all changes are appropriately monitored. Any production deviations are appropriately triaged and resolved.

Privacy

Introduction

Castlight maintains a comprehensive privacy program to ensure the proper use and protection of personal information, preserve privacy fundamentals, and allow for meaningful choices in the way customer data is collected and used. We work to earn our customer's trust by fostering privacy principles and best practices related to data protection.

Laws & Regulations

Castlight is compliant with regulatory requirements such as California Consumer Privacy Act (CCPA) and General Data Protection Regulation (GDPR).

The Privacy Team establishes privacy and data protection policies to standardize definitions for privacy and data, create minimum uniform safeguards for business activities and create processes for third parties that Castlight shares data with.

Individual Rights

Castlight has established and implemented processes for executing individual rights pursuant to applicable laws, including CCPA and GDPR. Castlight end users are able to exercise their individual privacy rights to know, access and deletion by contacting us.

Privacy Shield

The Privacy Shield Framework to provides companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data in support of transatlantic commerce. While the future of Privacy Shield is unsure, the evaluation serves as a useful tool to measure maturity and support basic privacy principles.

For more information, please refer to Castlight Status.

Privacy Policy and Statement

Our Privacy Policy and Privacy Statement is regularly updated and available on our website.

Compliance

Introduction

Castlight maintains a robust compliance program built upon industry-standard certifications. We understand that security requirements are top priority for our customers, and as such, we work to ensure our services comply with recognized certifications and regulations to address security risk.

Program Overview

Audits and Assessments

Castlight regularly undergoes independent verification of our security, compliance and privacy controls. While not a comprehensive list, the following certifications provide a robust view of our routine evaluation by independent external parties.

SOC 2 Type II

Annual attestation of Trust Service Criteria of Security, Availability and Confidentiality. Interested parties can request a copy of most recent report.

External Penetration Testing

An annual review that our applications are adequately protected from unauthorized access and are free of common security defects, such as those in the OWASP Top 10 and CWE/NIST Top 25 Most Dangerous Software Errors. Interested parties can request a copy of the most recent report.

SOX 404

As a public company subject to SOX 404, Castlight's IT environment is reviewed for general and application controls in support of our financial audits. Interested parties can review our publicly available financial statements for more information.

Risk Governance

The Castlight Risk Committee is comprised of top leadership of the company. The Committee is responsible for the oversight of Castlight's security, privacy and compliance programs and risk management activities.

Policy and Procedure Management

Castlight has a comprehensive set of security, privacy, and compliance policies. All policies are reviewed annually, require Executive approval and require annual review and acceptance by affected employees.

Conclusion

Trusted by hundreds of employers, Castlight is committed to investing in our security to allow you to invest in your company's health and wellbeing.

The protection of your data is a core consideration for Castlight's infrastructure, development and personnel operations. We hope this guide has provided a high-level understanding of our commitment to curating a robust security program. For further documentation and requests, please reach out to your account representative.