User security and privacy is Castlight’s #1 priority

To protect our users’ information, Castlight Health invests in industry-leading protocols and processes.

Our servers are secured in accordance with industry standards
Castlight is hosted in a secure server environment. That means the data center we use is both physically and electronically secured. Facility physical safeguards include restricted access to authorized personnel, entry regulated by biometric scans, and security camera surveillance monitoring. Castlight’s corporate facility also utilizes physical security controls to restrict and prevent unauthorized access. Our platform servers are protected on the Internet behind a firewall, which blocks access by unauthorized parties. Castlight’s infrastructure is configured for maximum security, employing least port access, traffic load balancing for server masking, network switching with VLAN segregation, host intrusion detection systems (HDS), server function segregation (web/application, database), and Linux (protected kernel) base operation system (RHEL).

Data protection is important to us
Castlight encrypts application data in transit and at rest, and actively employs data leakage protection (DLP) mechanisms. Files from customers and data partners are sent in batches through secure file-transfer processes (SFTP) and encrypted with PGP at rest. Data in transit is encrypted through HTTPS via a SSL certificate. Data at rest is encrypted through AES 256 bit encryption.

Signing in is safe
When you sign into Castlight using your browser (ex. Microsoft Internet Explorer, Mozilla Firefox), Transport Layer Security (TLS) technology protects your information using both server authentication and data encryption to help ensure that data is safe, secure, and available only to the correct user.

Accounts are locked against intruders
Castlight requires that a user enters his/her unique user name and password for direct logins. After a series of failed authentication attempts for a specific user account, that account will be temporarily locked. This helps protect against the loss, misuse and unauthorized alteration of data, and supports Castlight’s broader network intrusion detection systems (NIDS).

We partner with leading authorities
Castlight, its employees and its practices follow HIPAA guidelines. Castlight has also partnered with security leaders McAfee and VeriSign to ensure ongoing adherence to the strictest security standards in the industry.

We have a team dedicated to your security
Castlight has a dedicated team of security professionals that make sure data is always protected. These security professionals perform information, vendor, product and customer security reviews. Internal security and compliance audits are also performed to improve operations.

LEARN MORE
Castlight Security Policy
Visit www.castlighthealth.com/security
Email security@castlighthealth.com
Privacy support 1-888-226-8021

Castlight Privacy Policy
Visit us.castlighthealth.com/privacy
Email privacy@castlighthealth.com
Toll-free compliance hotline 1-855-754-2917