Security Statement

SocialCare employs many different tactics to protect information from theft, misuse, unauthorized access, disclosure, alteration, and destruction.

All SocialCare computer systems are protected by user authentication, file system encryption, malware prevention/anti-virus, firewalls, and host based intrusion detection. All systems are audited for primary function and any unnecessary software, services, and/or OS features are either disabled or uninstalled. System logging is sent to a remote, secure, and segmented management host server which parses logs nightly then forwards any possible issues to SC system administrators. External transmission of all information to and from our platform is secured via Transport Layer Security (TLS) protocol which encrypts the data and prevents eavesdropping and tampering. Protected health information is never stored on mobile devices.

The data center provider that houses SocialCare's development and staging environment is an enterprise-class SSAE 16 / AICPA SOC 2 Type 2 certified Data Center which is audited, and meets the most stringent compliance requirements mandated by HIPAA, PCI, SOX, FISMA, FERPA, GLBA, Safe Harbor and more. The data center has been purpose-built with a hardened single-story structure and fully redundant infrastructures (power and connectivity) to support the continuous operation of hosted mission critical assets. Facility design and construction provide assurance that operations are protected against unauthorized access, fire, floods, high winds, power outages, network issues and other hazards. For fire prevention the facility is free of flammable materials, use Pre-Action pressurized air-dry pipes with two sensors required to release water, and are exempt from power off during a fire event. Physical security is handled with layered access controls (FOB, PIN biometrics), anti-tailgating mantraps, access record retention, and closed circuit TV. Visitors are authenticated in mantraps, a process in which the data center personnel match photo ID with records of authorized visitor lists. Visitors that are authenticated must surrender their photo ID to the NOC personnel before being granted access to the Data Center and escorted by a member of the NOC staff to their equipment. As an outside hosted data center they are regularly scrutinized on their physical security by third party experts.

SocialCare does not store or process credit card information.

SocialCare undergoes an annual 3rd party security assessment and a bi-annual accreditation that evaluates our security protocols. All SocialCare employees undergo annual training on security procedures as well as HIPAA Privacy and Security policies.

Contact Us: If you have any questions regarding this Security Statement, please contact us at info@socialcare.com.