Application Hosting, Data Security & Privacy Overview

Introduction

CHESS Health has five years of experience in delivering its technology solutions for behavioral health and utilizes industry best practices with respect to data security and operational controls. All data is encrypted in-transit and at rest. Complex passwords, auto-logouts, role-based security, and segregated databases control access to patient data. Intrusion detection, vulnerability scanning, virus protection, and penetration testing protect the networks and devices used by CHESS employees and the solution databases hosted at Amazon Web Services (AWS), which itself has the industry's most advanced physical controls protecting their data centers. Organizationally, CHESS limits access to production systems, limits access to patient and customer data, ensures all devices are encrypted, and the company has strong methodologies and written policies spanning all aspects of its hiring, training, engineering, customer support processes relevant to data and system controls. CHESS Health expects to receive HITRUST Certification of its controls in the first half of 2021.

Furthermore, CHESS understands the importance of being a good steward of its customers' data, which includes sensitive patient data. Our contracts specify that our customers retain ownership of their data – CHESS never uses or re-sells any data other than using de-identified data (in accordance with Section 164.514(a) of the HIPAA Data Security Rule) for the purpose of internal usage analytics and to offer all customers blinded data for benchmarking their use of the CHESS solutions. Upon termination of a contract, CHESS will dispose of a customers' data (per our agreement, customers may request an extract(s) of data prior to termination, if desired).

In its five-year history, CHESS has never had a breach of its systems nor a release of patient data. What CHESS has learned and proven in five years is how to build and implement an advanced platform to address the crisis of substance use disorder (SUD) and other behavioral health disorders in the United States and internationally.

Answers to Frequently Asked Questions (FAQs)

Application and Data Hosting

- *Where are the CHESS solutions hosted?*
  The CHESS solutions are hosted at Amazon Web Services (AWS), with the primary environment located at an AWS data center in Oregon and a backup environment, for redundancy, in Virginia.

- *Is any customer or patient data stored outside of the United States?*
  No

- *Is any customer or patient data stored on servers in the CHESS offices?*
  No

Encryption

- *Is customer and patient data encrypted in transit (when sent over the Internet)?*
  Yes, CHESS uses 256bit AES encryption for encrypting data in transit

- *Is customer and patient data encrypted in storage?*
  Yes, CHESS uses TDE (Transparent Data Encryption) in its databases; no data is stored unencrypted.

333 West Commercial Street, Suite 2500, East Rochester, NY 14445 844 MY-CHESS (692-4377) www.chess.health

- *Are encryption keys stored in a FIPS 140-2 Level 3 compliant Hardware Security Module (HSM)?*
  Yes, CHESS uses Amazon's Key Management Service (AWSKMS) which meets this requirement

Data Security Tools & Services

- *Does CHESS employ intrusion detection?*
  Yes, CHESS uses AlertLogic for intrusion detection

- *Does CHESS employ vulnerability scanning? Will CHESS provide a vulnerability report upon request?*
  Yes, CHESS uses Qualys for vulnerability scanning and can share its report upon request

- *Does CHESS employ penetration testing?*
  CHESS is currently contracting with a third party to perform penetration testing

Organizational Controls

- *Where is CHESS located? Do all CHESS employees reside and work in the U.S.?*
  CHESS is located in Rochester, NY. All employees are U.S.-based.

- *Does CHESS outsource/use third parties for development or customer support activities?*
  No, CHESS doesn't outsource/use third parties for this work. Only the marketing team uses outsourced services (U.S.-based) who don't access CHESS systems or engage with customers or patients.

- *Does CHESS limit employee access to production systems to only those requiring access?*
  Yes, CHESS has strict controls on employee access to production systems and customer data.

- *Does CHESS perform background checks prior to hiring new employees?*
  Yes

- *Do all CHESS employees sign data confidentiality agreements and get annual HIPAA training?*
  Yes

- *Does CHESS use specialized training and testing related to phishing and other employee vulnerabilities?*
  Yes, CHESS uses KnowBe4 for accessing company security risk and for specialized phishing training, including random tests of employees.

User Controls

- *Do CHESS solutions employ role-based access, limiting users to functions and data based on their roles?*
  Yes

- *Do CHESS solutions enforce password complexity and auto-logoff functions?*
  Yes

333 West Commercial Street, Suite 2500, East Rochester, NY 14445 844 MY-CHESS (692-4377) www.chess.health

- *Do CHESS solutions require a user to create a new password upon first login?*
  Yes

- *Do provider/staff users accessing the web-based dashboards to the CHESS solutions need to download any software to their desktop/laptop computers?*
  No, the CHESS solutions run on Google Chrome and Safari browsers.

- *Do provider/staff users using the CHESS solutions need to use a smartphone?*
  No, smartphone use for the provider/staff is optional. The provider/staff functionality is available via a web browser or a smartphone app.

CHESS Policies and Certifications

- *Does CHESS have a documented Information Security Plan?*
  Yes

- *Does CHESS have a documented Security Incident Response Plan?*
  Yes

- *Does CHESS have a documented Disaster Recovery and Business Continuity Plan?*
  Yes

- *Is the Disaster Recovery Plan tested annually? What is CHESS' target Return To Operations (RTO) time?*
  Yes, CHESS tests its disaster recovery plan at least annually. CHESS's stated RTO time is under four hours.

- *Does CHESS maintain cyber insurance in the amount of $5,000,000?*
  Yes

- *Does CHESS have, or will it be obtaining, HITRUST certification?*
  Yes, CHESS will begin the process of obtaining HITRUST certification in the Summer of 2020.

333 West Commercial Street, Suite 2500, East Rochester, NY 14445 844 MY-CHESS (692-4377) www.chess.health