CarePortal

Security

1/10/20

Security and availability of CarePortal.org are of paramount importance. Industry best practices and HIPAA security rules have put the following safeguards in place for both our web application and phone based applications.

Data Extent

Minimum Case Data Collected
Our tools do not require significant case data to be entered, and can be utilized without entering any personalized information. Nonetheless, we take data security extremely seriously. Read our Privacy Policy to learn more.

Data Security

Encryption Everywhere HIPAA §164.312(e)(2)(ii), §164.312(e)(1)
We use strong browser encryption, encrypt data at every stage of transit, store data only in encrypted storage systems, and implement strong processes and procedures for managing the encryption keys. Sensitive information has an additional encryption layer at the application level.

Data Location

All Data In The U.S. - HIPAA §164.310(a)(1)
All data collected through our tools are stored in the United States. CarePortal data is stored in AWS US-West-2 Region - which is in Oregon. AWS data centers are SOC2 compliant and ensure there is no unauthorized physical access to servers and data.

Data Integrity

Secure Backups and Restores HIPAA §164.308(a)(7)(ii)(A), HIPAA §164.312(c)(1)
We have all data encrypted, mirrored and backed up using Amazon's Backup Services for daily, weekly, monthly and yearly backups. This data can be easily restored in case of an emergency. Policies and procedures are in place to ensure there are no unauthorized changes to underlying data.

Data Sharing

We do not rent, sell, or exchange our mailing lists and do not disclose your personal information to third parties.

Access Control & Authentication

Role Based Access - HIPAA §164.312(a)(1), HIPAA §164.312(a)(2)(i)
We use unique usernames for every user in the system and access to information is limited by role. Agency Workers can only view information about their requests, Agency Representatives about their assigned county, and Agency Executives can only view information relating to their agency. This hierarchy continues, granting additional access as needed up to the Global Administrator who has access to all requests and records.

Code Scanning

Automated Common Vulnerabilities and Exposures (CVE) Detection
We leverage advanced code scanning tools to ensure that the code we produce is free of known CVE issues. These tools automatically review every version of the software we produce, and are regularly updated with the latest vulnerability notifications.

System Architectures

We Scale So You Don't Have Too - HIPAA §164.312(b)
Our tools are specifically architected to achieve extreme scale and uptime. Configuration changes are limited by strict policies and procedures. This means every social worker can access our tools, and they do not have to worry about the availability of our services. This means we focus on technology so your organization can focus on children.

Want to review our security and architecture documents? Contact info@careportal.org.