Bonterra™

# SECURITY AND HOSTING

# Bonterra Classic Case Management

Bonterra Program Management (formerly Social Solutions) takes comprehensive measures to ensure that data is kept safe, confidential, and recoverable in the case of a disaster. Our software meets current HUD Domestic Violence, HMIS, and Social Security Administration data management and security protocols, as well as minimum required FERPA and HIPAA standards. Bonterra Program Management's office sits behind a ForcePointTM firewall which extensively controls, tracks, and reports access to our internal infrastructure.

## DATA SECURITY

Bonterra Program Management's Classic Case Management solution secures sessions with usernames and passwords to prevent unauthorized access and to restrict user access within the application. Each unique user account is assigned access to programs and permission sets to restrict access to data and features in the system. Customer data is housed in two locations (U.S. and Canada) based on the location of the client. Data is stored using redundant AWS hardware technologies and SSG fault tolerant software and journaling file systems.

## ENCRYPTION

Bonterra Program Management uses state-of-the-art equipment and technology to safeguard the confidential nature of your data Your data is automatically encrypted while in transit between your computer and our servers through Transport Layer Security (TLS). The encryption protocols and the cipher suites used to access ETO software meet the Federal Information Processing Standard (FIPS) 140.2 requirements. ETO software's data storage is secured by AES-256 while at rest.

## SOC2

Our SOC2 Type 2 (SSAE18) report is a comprehensive document that describes Bonterra's security controls in the domains of Administrative, Physical, and Technical security. Bonterra Classic Case Management is certified SOC 2 Type II compliant. Bonterra Program Management's security controls are reviewed by independent external auditors during audits for our SOC compliance.

## PASSWORDS

- can be set to have a minimum length
- can be set to contain non-alpha-numeric characters
- can be set to expire
- can be locked after a set # of invalid login attempts
- can be changed by a local administrator
- are not displayed upon entry and are encrypted

## AMAZON WEB SERVICES (AWS) SERVER SECURITY

Each of our servers is individually governed by a system that is designed to prevent unexpected Internet data from being processed by our server solution. IDS, virus scanning, automated system checks, and remote logging guard against unauthorized access. AWS implements electronic surveillance and multi-factor access controls to secure its data centers. Data centers are staffed 24x7 by trained security guards, and access must be strictly authorized. The AWS database utilizes object-based storage in the form of backups to S3 in encrypted folders. Multiple availability zones allow Bonterra Classic Case Management to remain resilient in the face of most failure modes, including natural disasters or system failures[1]. In case of a disaster at the AWS East region, Bonterra Program Management will have the solution up and running between 24-48 hours at the AWS Oregon region. The disaster recovery process is tested annually.

## REDUNDANT INFRASTRUCTURE AND BACKUPS

- 24/7/365 monitoring of uptime across the infrastructure
- Redundant water, power, telecommunications, and internet connectivity to maintain continuous operations
- Fully redundant SAN access storage and daily AES-encrypted full backups

## RETENTION POLICY

- Keep daily backups for seven days
- Keep weekly backups for six weeks
- Keep monthly backups for twelve months
- Keep yearly backups for one year

## COMPLIANCE

The AWS cloud infrastructure has been designed and managed by Amazon.com. AWS adheres to:

- SOC 1/SSAE 16/ISAE 3402 (formerly SAS70)
- SOC 2
- SOC 3
- PCI DSS Level 1
- ISO 27001[2]

[1] For additional information visit: https://aws.amazon.com/whitepapers/overview-of-security-processes/
[2] For additional information visit: https://aws.amazon.com/compliance/pci-data-privacy-protection-hipaa-soc-fedramp-faqs