2020 Information Security Overview

Data Security

- Security Awareness Program provides annual training, security advisories, and a Security Champions Initiative
- All PHI/PII data is encrypted at rest and in motion
- Automatic alerts and encryption for emails containing PHI/PII
- Third-party Information Security Risk Assessment is performed regularly

Endpoint and Systems Security

- Protection on laptops and workstations includes USB drives disabled, anti-virus installed, and full disk encryption
- Anti-virus installed on servers
- Databases are encrypted
- External vulnerability scans performed monthly along with laptop and workstation patches

Access Control

- Password best practices followed
- Multi-Factor Authentication (MFA)

Third Party Security

- Vendor Management Program verifies all third-party access to our systems
- All vendors or third parties required to complete security risk assessment periodically

Network Security

- Network access control for LAN ports and WiFi
- Web content filtering and firewalls
- Penetration testing semi-annually

Application Security

- Data masking of sensitive data with role based access
- Release management includes OWASP security testing and a full technical committee review
- Agency Workspace provides secure business case submission

Business Resilience

- Disaster Recovery Plans tested annually
- Back-ups verified to meet Data Retention Policy
- Incident Response Plan tested annually

Certification and Attestation

- SOC 1 Type 2 and SSAE 18

Physical Security

- Physical access to data centers only for authorized employees and visitors with ID and BenefitMall escort

BenefitMall
NEXT GENERATION BROKER SERVICES

20200323A 1897 B