Data Security

Accushield is SOC 2 Type I certified, demonstrating our commitment to the highest standard of data security and privacy. This certification verifies that our systems and processes are designed to keep your information secure.

Systems Protection

No data is stored locally on Accushield employee machines

- All data is stored on Google cloud, Amazon S3, or in the RDS database hosted on Amazon Web Services (AWS) cloud
- The Kiosk is secured with an MDM (mobile device management) software
- The data from the kiosk or community portal is transferred securely to the cloud using HTTPS
- The Kiosk is designed and installed in a secure way, minimizing the chance of theft

Systems Safety & Security

The Accushield system is hosted in the Amazon Web Services (AWS)

- WAF and AWS Shield have been configured to block unnecessary traffic and protect from DDOS/ SQL injection attacks
- Centralized logging, reporting, and analysis of logs provide visibility and security insights
- Vulnerability and Penetration testing is performed annually by a third party security team
- Strong Change Management policies and enforcement are upheld
- A system uptime of 99% has been maintained over the period of the last 3 years

https://aws.amazon.com/compliance/

Personal Data Protection

Only minimally required personal data is captured from the Kiosk

- The captured personal data is stored in encrypted format in the RDS database hosted on the Amazon Web Services (AWS) cloud
- The credentials of service providers and vendors are verified by our staff who are trained inpersonal data protection, HIPPA, GDPR and KYC rules and regulations
- The validated documents are encrypted and stored in AWS S3
- Continuous data protection is enabled on the RDS database and snapshots are stored securely in AWS S3

Password Management

Clear password management guidelines have been established for employees and the IT infrastructure

- All employee passwords are required to be changed every 60 days and the last 6 passwords can't be repeated
- All employees must set strong passwords which are at least 8 characters long and a combination of uppercase letters, lowercase letters, numbers, and symbols
- As an additional layer of security, MFA is mandatory for all the employees
- The same applies to all the IT infrastructure
- SSO and MFA are required to access infrastructure
- Employee access to all systems is revoked automatically on their last working day
- Access to production environment is strictly managed

We are proud to maintain a Soc 2 Type I for the safety and security of our customers'private information. If you have any questions regarding data security or would like torequest a copy of the full report, please reach out to **techsupport@accushield.com**.