# Protecting Your Business and Employee Personal Information
# Security & Technology Protocols

The justification for the need to implement stringent security measures arises from the fact that computer hackers specifically target personal information, including banking and health-related data. In this context, it becomes evident that PHSP, being a repository of all three types of sensitive information, necessitates a level of security far superior to that offered by two-step ID verification. The reputation of your organization, as well as the security of your employees, are at stake, underscoring the importance of upholding robust security protocols.

PHSPCanada technology and security protocols powered by myHSA software includes:

- AI Protection – Voice Calls / Fraud Calls
- Annual penetration tests and a full 3rd party GAP analysis based on ISO 27002.
- Apps for Android and IOS.
- AWS access uses MFA and whitelisted Ips.
- AWS WAF to protect against SQL injections, geo restrictions, etc.
- Chief Information Security Officer (CISO) is on the D team.
- Client Data is stored on the cloud in AWS in Montreal, Canada.
- Client sensitive information is encrypted using Rijndael 256.
- Cloud CloudWatch and CloudTrail to monitor our EC2 instance on AWS.
- Dark web scanning and monitoring.
- Environments are physically segregated based on advisors our builds go through 3 levels of testing (development, QA environment, Staging).
- IT policies are based off of ISO 27002.
- SIEM as a third party provides 24 / 7 monitoring.
- SOC2 certification on October 31, 2021.
- Source control is stored and maintained in GitHub. With 3 levels of encrypted backups including daily on production, the last 2 days on S3, the last 2 weeks on Staging.
- Third party quarterly Application Assessments.
- Two step ID verification
- Website uses an SSL certificate.

**Ensuring the integrity of our systems against external threats is of utmost importance.**