As custodians for your data, POLAR lives and breathes security in every aspect of its daily operations

Therefore having the correct security posture is paramount to ensuring the platform's success and maintaining the valuable relationship between Primary Health Networks (PHNs) and General Practices (GPs).

This Q&A sheet has been designed to provide a high-level overview of the most common security/data questions. If you need to know more, please feel free to contact us using the details at the bottom of this fact sheet.

> "The ability for practices to audit their data and identify improvement is integral. POLAR stands above the rest to help ensure continuous quality improvement and improve patient outcomes."
>
> **Alex Dolezal**
> **Digital Health and QI Team Leader**
> Central Eastern Sydney PHN

Q&A

Infrastructure

What type of Cloud is the System running in? (Azure, AWS, Private Cloud)
Private cloud - Colocation (Australia based)

Colocation / Datacentre Certifications
- SOC 1 Type II
- SOC 2 Type II
- ISO 27001
- ISO 22301
- PCI DSS

Is all data stored in Australia?
Yes. Data never leaves Australian shores. Outcome Health also enforces GeoIP restrictions so the web based applications cannot be accessed outside of Australia.

Is the data held by Outcome Health encrypted?
Outcome Health applies data encryption in multiple layers, including but not limited to during transmission and at rest.

Do you have backups?
Yes. We take regular encrypted backups, of which we keep 2 copies onsite, and a copy offsite in a secure location.

Do you regularly patch your systems?
Yes. Outcome Health has an automated patch management system. Systems are patched on a regular basis, or when required after security vulnerability announcements.

Who has access to the environment ?
No third parties have access to the patient \ clinic data. Formal agreements are in place with any third party that may be required to access the environment.

What Security Controls are in place such as intrusion detection systems ?
- CloudFlare WAF - Web Application Firewall, the first line of defence for threats arising from the internet.
- Firewall - Intrusion Detection \ Prevention System
- Security events and Information Management (SIEM) - Centralised logging and alerting across all network and infrastructure systems.
- Security Operations Centre (SOC) - Outcome Health has partnered with an Australian based security provider to provide network monitoring services across all of Outcome Health systems. They also conduct quarterly threat hunts, actively monitor for anomalies and security events, including 0 day attacks.

Want to know more? Contact us on:
(03) 8822 8433 or
support@outcomehealth.org.au

POLAR

Fact Sheet: POLAR Data Security

How is client data segregated from other client data?
Within POLAR each practice has their own unique landing database. This is not accessible by other clients. The POLAR portal restricts access to resources based on the organisation, user type and role. i.e. a clinic can only see the reports for that clinic, provided that the user has been granted access to the report. A PHN cannot see a clinic report, and are restricted to reports specific to their PHN.

How are Security and Privacy incidents handled?
Outcome Health has policies in place covering data security breach events, and recovering from such incidents. Our aim is to remain as transparent as possible.

Application Level

Does Outcome Health conduct 3rd party audits and penetration testing?
Yes. Outcome Health as an organisation holds ISO 9001 certification. POLAR undergoes yearly NIST CSF control reviews, as well as penetration testing across all key applications. Additionally, Outcome Health external Security Operations Centre (SOC) undertakes quarterly threat hunts looking for threats or suspicious activities across the internal environment.

Can the application authentication process be integrated with client identity and access management process?
No. We are currently exploring ways to enhance existing authentication systems allowing integration of external IDAMs via SAML.

Is Multifactor authentication a standard offering?
Yes. Multi Factor Authentication (MFA) is mandatory for Outcome Health (OH) and Primary Health Network (PHN) staff. MFA is available for General Practices (GP) on request.

How is Security allocated within the application in terms of job functions / roles?
Outcome Health has a dedicated ICT Security Specialist role, however security is a core function and consideration across all teams and their roles. Outcome Health provides security and privacy training to all staff so everyone is well informed when handling patient data. Outcome Health also has a dedicated 3rd party Security Operations Centre (SOC) that monitors for any internal and external threats.

Are User Access Logs available ?
Yes. We collect user access logs across our web based applications.

Do users need to have Domain or Local Administrator rights on their local machines to run the application ?
Hummingbird data extraction client requires local administrator rights to be installed, however day to day operations do not require admin rights as the POLAR portal is web based.

Systems Support

Do you provide phone and email support?
Yes. POLAR provides a service desk functions Monday to Friday, 9AM to 5PM AEST excluding public holidays. Tickets can be raised 24 hours a day in the dedicated support portal.

Data & Privacy

Do you comply with the Privacy Act, including the Australian Privacy Principles (APPs)?
Yes.

Is the data collected, protected?
Outcome Health utilises various different types of encryption and data protection technologies to protect the data. This means that we mitigate risk from extraction through to transmission, storage, user access and dissemination.

Do you have a privacy policy?
Our Privacy Principals can be viewed here:
https://www.outcomehealth.org.au/privacy-policy/

How do you securely handle data?
We are the custodians for Primary Health Network data, which is a responsibility we take very seriously and manage by adhering to the following standards and protocols that are guided by key principles, including:

- Sensitive information must be encrypted
- Strength of cryptography corresponds with information classification levels
- Cryptographic keys must be securely managed
- Use only approved cryptographic algorithms

Do you access identifiable data?
No. All data is de-identified before it leaves the practice

Do you have ethics in place?
Yes. Data handling and management (including collection and de-identification) on the POLAR platform has ethics approval from RACGP NREEC (Protocol ID: 17-008).

POLAR

Want to know more? Contact us on:
(03) 8822 8433 or
support@outcomehealth.org.au