POLAR is an end-to-end data analysis and reporting solution designed and developed by Outcome Health. For general practices, POLAR enables meaningful analyses of your identified patient data through a user-friendly graphical reports.

Data Security and Privacy

Outcome Health takes data security seriously. We go to every effort to ensure your patients identifying information is not taken offsite from your practice. We are constantly updating and reviewing our security protocols to ensure legislative and best practice compliance in line with ISO27001 standards. Data security encompasses three distinct components for Outcome Health

- access to the IT hardware that stores data processed from stakeholders (data warehouse);
- the development of the POLAR applications and tools that facilitate interaction with the data; and
- independent external IT security auditing to ensure compliance with international best practices.

How does POLAR manage your data?

Figure 1 demonstrates the POLAR data management process. The POLAR data extraction tool starts the data collection (extract). This data is de-identified, and encrypted using industry endorsed algorithms similar as those used in the health, banking and e-commerce sectors. This encryption ensures that data transmission (uploading) of the de-identified data to the POLAR data warehouse is safe and that a patients' privacy is protected at every step of the process.

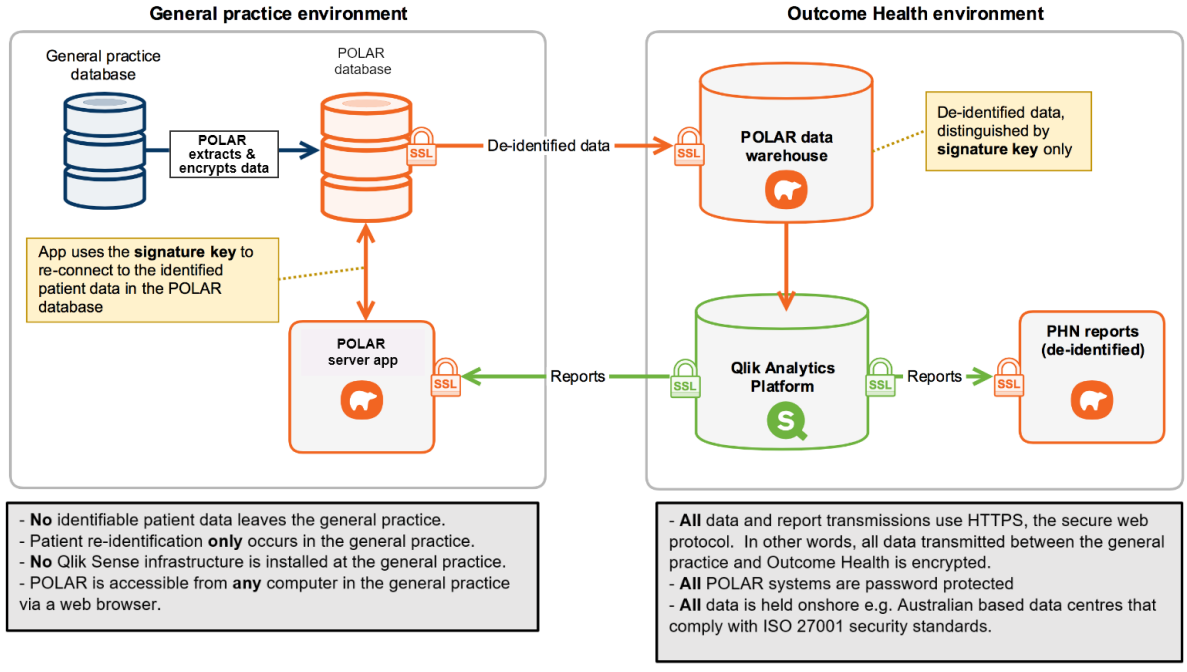

Figure 1 – POLAR data management process

The POLAR GP server app allows the practice to use browser based reporting and still realise all the benefits without any identifiable data leaving the practice. According to a schedule determined by each practice, POLAR will automatically collect (extract) data from both the general practice's clinical and practice management software.

Where data is aggregated for PHNs population health or research purposes, each patient's data is standardised into coded datasets (for quantitative analysis), and any free text fields (i.e. qualitative data) are omitted. If there is a diagnosis that has been entered as free text, POLAR's extensive SNOMED mapping tables will endeavour to match it to its coded equivalent.

Hardware Access

All data stored on Outcome Health servers is de-identified. Only encrypted patient information leaves your site and is stored by Outcome Health. All server access is restricted to IT administrators who have relevant police checks and contractual obligations around data. The physical servers are located within an access controlled server environment. All IT infrastructure is actively monitored and maintained by an independent ISO27001 compliant IT security experts, which in conjunction with Outcome Health, ensures that all hardware is up to date with relevant software and security patches to protect from any malicious attack.

Software Development

The POLAR software development team follow standards set out by the Open Web Application Security Project (OWASP) that establishes secure coding practices to achieve the best possible results in software quality, reliability and security. Best practice software development exercised by the POLAR development team requires:

- All data stored or transmitted is encrypted;
- All administration and server access requires multifactor login e.g. login to network are separate to server administration;
- POLAR software is internationally certified and code signed with internationally recognised anti-virus software.

IT Security Auditing

Outcome Health undertakes external security auditing by a leading international security company, eSecurity Solutions. The assessment includes:

- Security Review & Gap Analysis, which produces a risk profile along with a Discovery Risk Score; and
- Security Testing, that incorporates the testing of all internal IT security procedures along with external penetration testing of all IT systems.

Handling of Security Breaches

While no method of transmission over the Internet and electronic storage is perfectly secure, and absolute security cannot be guaranteed, if Outcome Health learns of a security breach, we will notify relevant affected users so that they can take appropriate protective steps.

Your Responsibilities

Keeping your data secure also depends on you ensuring that you maintain the security of your own systems. This includes, keeping up to date with the latest release of POLAR, notifying us of any security issues you become aware of at your practice, whether they be POLAR related or not. Being open about security allows all parties to ensure optimal security is proactive and remains a top priority.