# How does POLAR manage your data?

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 user-friendly graphical reports.

Figure 1 demonstrates the POLAR de-identification process. The POLAR data extraction tool starts the data collection (extract). This data is de-identified, and encrypted using industry endorsed algorithms similar to 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.

# Data security and privacy

Outcome Health takes data security and privacy 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 international standards.

For more information about POLAR data security and privacy please refer to the document below or contact support@outcomehealth.org.au

<https://www.outcomehealth.org.au/megpn_upload_folder/sitedocuments/polar%20security.pdf>

# What is data de-identification?

According to the Office of the Australian Information Commissioner:

“De-identification of personal information can enable information to be shared or published without jeopardising personal privacy. This enables organisations to maximise the utility and value of information assets while safeguarding privacy and confidentiality.”

“De-identification involves removing or altering information that identifies an individual or is reasonably likely to do so. Generally, de-identification includes two steps:

1. removing personal identifiers, such as an individual’s name, address, date of birth or other identifying information, and
2. removing or altering other information that may allow an individual to be identified, for example, because of a rare characteristic of the individual, or a combination of unique or remarkable characteristics that enable identification.”[[1]](#footnote-1)

Figure 2 demonstrates the process of how the patient name data is de-identified by POLAR before uploading data to the data warehouse.

Figure 2 - Patient signature HASH key creation



The process for creating a patient signature HASH key

1. A FINAL KEY is created for each patient by taking information from their demographic information.
2. Once generated, the FINAL KEY data is scrambled (or hashed) creating the SIGNATURE HASH KEY. The non-demographic data is linked to the SIGNATURE HASH KEY ready for uploading.
1. Office of the Australian Information Commissioner (OAIC). Privacy business resource 4: De-identification of data and information. Accessed Friday 10 June 2016. https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-4-de-identification-of-data-andinformation. Australian Government. Sydney, Australia. [↑](#footnote-ref-1)