Policy: Privacy policy

ORGANISATIONAL PRIVACY POLICY: POLAR

Introduction

The Privacy Act (1988) was introduced to promote and protect the privacy of individuals.

Outcome Health takes your privacy seriously. This Policy outlines the privacy handling practices of Melbourne East General Practice Network, trading as Outcome Health (ABN 86 129 637 412) in dealing with personal information.

This policy sets out the principles that Melbourne East General Practice Network, trading as Outcome Health ("the organisation") has adopted in order to protect personal information and comply with privacy obligations. These principles deal with the entire lifecycle of such information including: collection, use and disclosure, access to, correction of, security and disposal.
The Organisation aims to ensure a high standard and compliance of documentation within its current practice and to strengthen information handling procedures in a way that is ethical and consistent with Commonwealth and State legislation.

The Organisation is committed to the protection of privacy (including health information) and has adopted a set of privacy principles based on relevant state and federal privacy laws and adherence to a range of existing legal and ethical obligations regarding privacy, security and confidentiality of personal information.

About this Privacy Policy

This policy has been prepared in March 2015 and reviewed yearly in accordance to Australian Privacy Principles (APPs). The APPs are found in the *The Privacy Act 1988* .
We collect personal information that is necessary to undertake our programs, activities or functions; these include facilitating the exchange of information between Outcome Health and other agencies.

Any enquiry or if they have a complaint about privacy or confidentiality should, in the first instance, be directed to the Organisation:

CIO
Role
8
8
2
2
8
4
44
Emai
l :
polar@
outcom
ehealth
Phone: .org.au

The organisation will respond to all privacy enquiries within 30 days, if a response is not received (after 30 days), then a complaint may be lodged with the Office of the Australian Information Commissioner (OAIC) on the enquiries line 1300 363 992 or, if calling from outside Australia call: + 61 2 9284 9749.

What is personal information?

Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable: whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not.

When do we interact with data?

Outcome Health offers a system called POLAR to General Practices. POLAR allows the practice to interrogate data in their clinical systems for a range of clinical improvement and population health based activity.

We de-identify this information and supply it to Primary Health Networks (PHNs) so they can use the data to commission services and provide quality improvement activity across their catchments. PHNs do not access identified data about you. You can read more about the PHNs roles here.

What types of personal information do we collect and store?

We collect clinical and demographic information generated and stored in your General Practices clinical information system. Your identifiable data remains with the practice at all times. We only store de-identified information.

Identifiable information about you is stored at the practice to ensure your care is coordinated in the best way. We extract de-identified information from the practice and make it available to PHNs.

We collect information that relates to the care you receive in the practice.
Data is collected in 11 broad categories:

- Demographic;
- Activity (number of visits and interactions);
- Medicare billing information;
- Diagnosis:
- Medications;
- Observations (height, weight etc)
- Pathology tests;
- Radiology tests;
- Immunisations;
- Cervical screening;
- Referral categories

Before the data leaves the practice, POLAR software allocates a unique encrypted key to each record. The key allows us to link data with other de-identified datasets to form a more complete picture of a patient's health journey.

The key is made up of fragments of personal information of each patient. Then it is encrypted and comes with the data to us. What we see is a meaningless combination of characters. We cannot reverse engineer the key to reveal any personal information about you. Here is an example of a key:

'0x1F7F84C948CA85E443B2F9FGFLKJA897ADS899E30C7FAC236585C679456FB782E9A3734B7679B'

It is not possible to re-identify a person from this information.

Can patients opt-out of sharing de-identified data?

Your practice only collects the type of information required to ensure you receive the best care possible. If, however, you would prefer your data to be excluded from quality improvement activities, your practice has measures in place to ensure your wishes are respected and adhered to.
When you visit your practice, you can inform the practice staff (receptionist, nurse or doctor) that you do not consent for your data to be collected. Your practice will then ensure your de-identified data is not shared with us.

Patients who do not consent to have data collected about them are entitled to receive the same level of high care so you can rest assured that your choice not to participate in data programs will not directly or indirectly affect the care you receive.

How do we collect data?

When you see your doctor, during the consultation they add information to your record in the practice's clinical IT system. The practice's POLAR software captures some of that information, de-identifies it and sends it securely to us. We clean and optimize it and then send it back to the practice. (Further detail in *' Why do we collect, hold and disclose data?'*)

The practice can view your details in their system, much like in the clinical system in the consultation room.

Before data leaves the practice, all identifiable information is removed so that only a de-identified subset of patient data is saved in our warehouse. The data in this warehouse is a tool which allows your Primary Health Network to design population health initiatives to improve the health of your community.

How do we store data?

We store de-identified practice data in a secure data warehouse. Your identified data does not leave the general practice. Practices can view your data only in their facility when they log in to the secure POLAR system.

Some parts of your de-identified data is viewable to the PHN in your region. PHNs use this data to know what services are most needed in your area and then work to address those needs.

Access to the de-identified data is strictly monitored, audited and restricted. We take all steps necessary to ensure your data is never accessed by an unauthorised person.

We have multiple levels of security to ensure we maintain highest standards of practice in how we handle your data.

Why do we collect, hold and disclose data?

Outcome Health does not disclose data to overseas researchers or other recipients. All POLAR data stays (and is stored) in Australia to:

1. Help general practices get meaning from their patient data

   First and foremost, we collect data to allow your practice to provide you with the highest possible level of care.

   Raw patient data is sometimes difficult to understand or use. When we extract de-identified information from practices, we clean it up and map it to standardised terms and then send it back. The practice's POLAR software then uses the cleaned-up data to give the practice insights about its patients. This information can help the practice improve patient care.

   For example, the POLAR software will make it easy for the practice to identify patients who are due for certain tests, like a patient with a heart condition with no cholesterol test recorded in the last two years or an older patient who is due for a health assessement.

   The POLAR software presents the data to the practice in easy to understand graphs and color-coded charts to make it easier to take practical steps to help their patients achieve best outcomes.

2. Help PHNs conduct evidence-based population health planning

   The PHN in your region assists the practice with their data management needs by providing advice and education. Practices are supported to use the practice data in a way which translates to tangible improvements in the health of their patients.

   PHNs access a copy of de-identified practice datasets which allows them to perform population health analysis. Your GP helps you manage your individual health needs and PHNs help manage the community health needs.

   For example, your PHN may identify an area with a particular health issue such as higher than average prevalence of mental health conditions for young people living in a certain region. It can then fund support services for people in that region. Without access to this de-identified data contributed by your practice, many of these needs would remain undetected and therefore unaddressed.

3. Support ethically-approved health research projects

   If your practice has agreed to allow research to be conducted on de-identified datasets, then a limited number of data items may be made available to researchers for PHN-approved projects. There are strict guidelines around which data items are available and for what studies. PHNs will only approve research that is ethically approved by an independent Ethics Review Committee and is of direct benefit to the general practice community. In some instances, your practice may choose to be involved in selected research. This ensures that medical knowledge is constantly improved which means that you continue to have access to best medical practice.

   Researchers cannot request access to all data items in the warehouse. In line with all other layers of security, research access is strictly enforced and monitored. Researchers access the data in a secure virtual environment controlled by Outcome Health.

   More detail on research activity can be accessed on www.polargp.org.au or by contacting Outcome Health on (03) 8822 8444.

How can you access your information?

You have a right to request access to personal information about you and to request that this information be corrected.

1. Access to your information

   POLAR is a population-based system, meaning that the primary emphasis is not on individual patients, rather it focusses on populations or 'groups' which may be at increased risk, for example: Asthma patients without a smoking status recorded.

   We collect de-identified information so we are not able to give you access to your information because we don't know which information is yours in the dataset.

   The best way to see what data POLAR collects, is by contacting your practice directly. You can access the information we collect at the practice by simply requesting to view it. To get a more complete picture of the type of information collected by your doctor during your visit, we recommend you request to see your medical record.

   Once de-identified the data is transferred to our secure warehouse, it is not possible for us to locate your record in dataset. Privacy is further protected by suppressing any cohort containing less than 20 patients. For example, patients with extremely rare conditions cannot be re-identified simply by searching for that condition if there are 20 or less patients in that group.

2. Correction of incorrect information

   For reasons described above, we can't correct your information. However, if you think your patient information may be incorrect (that is, the information that your doctor records during your visit), you can ask your doctor to correct it. That correction will then flow through to our database (albeit in de-identified form).

What are the risks?

Although the data we hold is de-identified, two broad risk categories remain:

1. An unauthorised person or agency accesses your data;
   or
2. A person or agency attempts to re-identify patients from the de-identified dataset we hold

Your privacy is our highest concern and we take important steps to ensure the risk of these events occurring is minimised.
We adhere to strictest security standards and comply with all relevant government legislation to ensure your data is protected at all times. In the rare event that a data breach occurs, we take immediate steps to contain and address the breach. We have a communication strategy in place to ensure potentially affected individuals are notified. For more information on our comprehensive Data Breach Response Plan, contact Outcome Health on (03) 8822 8444.

What is the complaints process?

If you believe a breach of the Australian Privacy Principles has occurred, you may raise your concerns or lodge a complaint with:

- Your general practice
- Your PHN

- Outcome Health - contact us on 03-88228444 and ask to speak to the CIO. Alternatively you can email us polar@outcomehealth.org.au

Complains are treated with highest priority and all reasonable steps are taken to address them. If you are unsatisfied with the proposed solution, you may lodge a complaint to an external body such as the Office of the Australian Information Commission.

Risk Assessment

This policy is assessed for risk of content variation and as such has the below rating:

Low Risk	Reviewed every 2 years
Medium Risk	Reviewed every year
High Risk	Reviewed every 6 months
Extreme Risk	Reviewed every 3 months or less