# Privacy Policy

## Purpose of this policy

EMPHN collects and holds information from individuals and organisations. We use that information to develop and support programs that will improve health outcomes for our community. However, handling personal information comes with risk that needs to be mitigated. This policy explains what information we collect and how we use it, what we share with other organisations, how we protect individuals' personal information.

## Scope of this policy

The policy covers:

- Personal, sensitive and health information EMPHN collects and holds from clinics and health organisations it works with
- Personal, sensitive and health information EMPHN collects and holds from health consumers
- Personal information collected and held from EMPHN employees, Board, committee and advisory body members

Everyone who works for and with EMPHN must treat personal information ethically; respecting individuals' privacy and confidentiality.

## Our privacy principles

This policy is closely aligned to the Australian Privacy Principles within the Privacy Act; and owing to the higher standards afforded to the sensitive and health information of health consumers, is also aligned with both the Commonwealth and Victorian Health Records Acts, and the Victorian Privacy and Data Protection Act.

It outlines our commitment to fulfilling our obligations and living up to our principles:

- We are transparent about what personal information we collect, and how personal information will be used, including secondary uses
- Prior to collecting personal health information, we seek consent; and explicitly define the primary and secondary ways the information will be used or shared
- Records of consent received are maintained
- Where appropriate, consent is sought from the consumer's carer, or guardian
- Where consent is not given, we only collect and use personal health information according to the Privacy Act and other relevant legislation, such as to prevent or lessen a serious threat to life
- Sharing or disclosing personal health information is directly aligned to the consent received
- Any use or disclosures of personal health information not consented to are made in strict accordance with the law, such as to prevent harm; and is done with appropriate protections in place.
- We have processes to protect people's privacy and their personal, sensitive and health information – with particular care for vulnerable health consumers; and cognisant of the needs of Aboriginal and Torres Strait Islanders, and consumers facing additional language or accessibility barriers, or difficulties stemming from complex health challenges

## Different types of personal information

EMPHN collects several types of information from our own workforce, from people and organisations we work with, from heath consumers and from visitors to our website. All information we collect is treated with respect, however we apply the greatest protections to individuals' personal health information, especially where that information can be identified as belonging to a specific person.

- Personal information – includes contact details that identify an individual
- Personal health information – includes information about an individual's physical or psychological status, health services provided to the individual, or an individual's expressed wishes about the future provision of health services
- De-identified information – information and data with all identifiable features removed
- Profile information – information and data with personal identifiable features (such as name, address and Medicare number) removed

## Why we collect personal information

**Personal health information**
This information is collected to understand a consumer's condition and need, and to provide advice, treatment, a referral or to follow-up with the consumer. Consent is always sought to collect this information; and to share it will the appropriate referral service where relevant.

**Deidentified health information**
EMPHN receives de-identified from the health services it funds and aggregates it with data from all over our coverage area to get a greater understanding of the health challenges of our community and the effectiveness of our programs. This aggregated and de-identified data is also commonly shared with other PHNs and government bodies to create approaches and programs across a wider geography or apply for funding based on the proven needs of our communities or groups within our population. We do not ask for consent to use this information for evaluations, but we ask consent from providers is this information is to be used for research.

**Profile information**
EMPHN and EMPHN funded providers also seek consent to share some personal health information from health consumers such as age, gender and postcode (but not name, address or Medicare number) with government bodies to better understand a health service's reach and performance and its value to the community. Consent is always sought and can also be withdrawn by the consumer at any time.

**Personal information**
Collecting information from our partners helps EMPHN provide health clinics within our catchment with the appropriate supports and quality improvements. It also means we can make informed decisions on which are the most appropriate clinics to invest in for a given health initiative.

EMPHN makes use of personal information to contact clinics and, and in some cases, health practitioners directly, to quickly and effectively disseminate the latest news on health trends or

make critical announcements, provide tools, explain changes to training requirements, or highlight funding opportunities.

Collecting and holding personal information also means EMPHN employs the right people with the right qualifications, experience, skills and personal attributes to work for us, on our Board, or in partnerships. HR and Payroll also use this information on an ongoing basis to manage employment or contract obligations.

**Website cookies**
When anyone accesses our website, we – via Google Analytics – collect metadata, which is considered personal information. Although EMPHN has no way of identifying individuals or their location from the data collected, it helps to understand what pages are of most interest to visitors and therefore ascertain what we should focus on. Information collected includes:

- your server address
- your top-level domain name (.gov, .edu, .com)
- date and time of access
- pages accessed and documents downloaded
- previous site you visited
- type of browser used

However, it is important to note, that if you fill out a form on our website, you are providing EMPHN with more information such as your name and contact details (if you provide them) and your location, along with whatever else you type in. This also applies if you respond to a popup asking for your location.

**Feedback**
EMPHN welcomes feedback. While there is the option for anyone to let us know their thoughts or experience engaging with us anonymously, to get a response and be kept informed of how we handle the feedback, we need both contact details and information about the commenter's role in the engagement. Information shared with us will be handled discreetly, and personal information will be protected and kept confidential, unless we get express consent to release identifying information. There is more about anonymity and providing feedback in our Feedback Policy.

## How EMPHN manages consent

When we ask consumers for their personal information, we explain how we plan to use it, and ask for their explicit consent for each way we plan to use their information.  NOTE: If consumers consent to sharing some of their profile information, such as age and gender, with the Department of Health and Aged Care, they can withdraw that consent at any time, and their information will be removed from the dataset.

Without consent to access and use a consumer's personal information, we can't provide some services, such as referring to an appropriate service, because we won't get a sufficient understanding of their circumstances to refer ethically. If a consumer declines to a request to

disclose their personal information, we explain how that impacts the health service that can be provided.

***Consent Handling Process for direct services***

When consumers contact a service delivered by EMPHN directly, our consent systems are overt – and involve both EMPHN and the service providers we might refer the consumer to. We ask consumers to share their personal and sensitive information to ensure appropriate and seamless transition between services, and to make sure they get the best care at each stage. To protect consumers and their information, these types of consent are sought:

1. **Agency Consent** is the consent EMPHN commission service providers take from consumers for providing health services.
   *To access a service commissioned by EMPHN a consumer must consent to provide their name and a way for a provider to contact them.*
2. **Consent to share profile data with the Commonwealth Department of Health and the Victorian Government Department of Health** allows sharing of a primary health minimum dataset with government agencies that supports health service planning and evaluations – that is, it supports continual improvement of the programs that EMPHN commissions
3. **Consent to the collection and sharing of all relevant information** with other services, carers and supports relevant to assist the consumer's overall provision of care – helps EMPHN and commissioned providers to offer high-quality, safe care for consumers
4. **Consent to the collection of information for the purposes of program evaluation** which supports continual improvement of the programs that EMPHN commissions.

## Can individuals correct information EMPHN holds about them?

If you believe EMPHN has inaccurate information about you, you can access the information EMPHN has under the authority of the Privacy Act (Australian Privacy Principles 12 and 13). And if you find information you think is false, you can ask for it to be corrected. If EMPHN refuses to correct that personal information, EMPHN must give you a written explanation saying why – and even in that case, you can write an amendment, which EMPHN must link to the record.

## Who we share personal information with

Information sharing happens across EMPHN's network of clinics, providers, programs and government departments.

- Personal information EMPHN collects is only passed on with the express consent of the consumer
- EMPHN ensures that information it receives from stakeholders has been collected with the appropriate consent from the consumer
- For de-identified patient data collected from GPs, EMPHN does not need consent for health service planning and evaluation activities; however; EMPHN requires consent from general practices to use de-identified data for research activities

- If there is a need for EMPHN to use data storage facilities outside of Australia – this will be managed to ensure the third-party is accountable to the same standards an Australian-based data storage facility holding health records is
- In some circumstances, EMPHN may be required to share personal information by either state or federal legislation

## Extra privacy protections for research and program evaluations

To understand the effectiveness of our programs in our community, or to get a clearer view of the gaps, we run evaluation programs that can involve collecting more personal information than we normally do. So, there are additional privacy protections in place during evaluations, especially for those which require an ethics review by a Human Research Ethics Committee (HREC). Privacy triggers for a review by a committee include:

- If the purpose of the evaluation is beyond quality improvement
- If the evaluation findings are to be published or presented at a conference
- If the activity potentially infringes the privacy of participants, providers or organisations
- Secondary use of data (that is, using data or analysis from quality improvement or evaluation activities for another purpose)
- Gathering information about the participant beyond that collected routinely
- Comparison of cohorts
- Targeted analysis of data involving minority/vulnerable groups whose data is to be separated out of that data collected or analysed as part of the main evaluation activity[1]

Any queries regarding ethical approval can be directed to the Evaluation Specialist.

## How EMPHN protects individuals' personal information

- Access to personal and health information is strictly limited to key roles within the organisation, such as HR and Payroll for employee information; and for consumers, to the specific Health Delivery team.
- Personal information provided by clinics is de-identified at the clinic level before it's given to EMPHN electronically; if EMPHN staff discover data that hasn't been de-identified, it's immediately destroyed, and we notify the clinic of the breach, and get them to fix the issue.
- Data security is managed by the Data Analytics team, and according to the Data Governance Framework, including setting and implementing standards for what and how data is collected, its management and access, and how it is shared with other government agencies.
- Disclosure of personal information is only allowed where legislation deems it appropriate and necessary, or for data storage with third-parties operating at the same level of privacy legislation and regulation as EMPHN.
- Whether documents are electronic, or in hard copy, all documents containing personal information of employees, other EMPHN representatives, stakeholders or consumers are stored

[1] Adapted from the National Health and Medical Research Council's Ethical Considerations in Quality Assurance and Evaluation Activities

securely; and where those documents contain personal health information, they are destroyed after seven years. All records are archived and destroyed in a timed and stepped sequence that prioritises personal information privacy.

- Contracts provide another protection. Business information must be kept confidential, both according to common law (law made by the courts), and as defined on contracts EMPHN has with our service providers. These contracts also address privacy, and specifically require privacy of personal, sensitive and health information be adequately protected by the organisations we work with, with effective safeguards in place.
- EMPHN's own employees have our personal and sensitive information protected in our employee contracts, and by several of our internal policies, such as our Code of Conduct.

## How we manage breaches

If there is a breach in EMPHN's defences and personal information is at risk, we follow our established Data Breach Response Plan to immediately stop the access or distribution, and protect the rest of the information we hold. At that point, we evaluate whether any breach of personal information is likely to result in serious harm to any individuals (such as physical, psychological, emotional, financial or reputational harm). And we assess whether remedial action can mitigate or remove the likelihood of serious harm.

In cases where there is a data breach involving personal information likely to result in serious harm, we follow the steps of the Notifiable Data Breaches scheme, and contact those impacted by the breach and the Office of the Australian Information Commissioner. If the My Health Record system is impacted, both the Australian Digital Health Agency and the Office of the Australian Information Commissioner (OAIC) are notified.

In step with our organisational commitment to continuous improvement, we review any breach and consider what can be done to prevent future breaches and minimise their impact.

## What happens to unsolicited personal information EMPHN receives

If EMPHN receives personal information that wasn't requested our standard process for managing that information is to destroy or de-identify it; and inform the provider of both the receipt and what's been done with the information. The same process applies to additional information we are given beyond what we've asked for. This may happen, for example, where requested de-identified information received from a GP clinic has some identifying details. Informing the provider is an essential element in limiting the chance of the same breach reoccurring. These events are also tracked in our risk system.

Exceptions to our 'destroy or de-identify' stance are in line with the Australian Privacy Principles, including if the information could have been collected via our standard ways of collecting personal information, or is already in a Commonwealth record. Where there is doubt, information is to be destroyed or de-identified.

Some personal information is protected by law from being destroyed or de-identified. One example is misdirected mail, which must be returned to Australia Post. Also, if the owner of the personal information is consulted and approves, such as a job seeker who sends a resume, HR can keep the resume on file for a reasonable period of time.

Ultimately, any unsolicited personal information EMPHN receives, or continues to hold, is afforded all the privacy protections outlined in this policy.

## Roles & responsibilities within this policy

**Chief Operating Officer**: Testing our privacy protections and management processes via EMPHN's Audit Series, and promoting overall staff awareness of the importance of privacy and their obligations. The COO is also EMPHN's assigned **Privacy Officer**, with responsibility to notify the Office of the Australian Information Commissioner where a breach might likely result in significant or long-term harm, as defined by the Office of the Australian Information Commissioner's (OAIC) Notifiable Data Breach Scheme.

**Managers**: Decisions about what information EMPHN needs, and how it is collected and held, are made with the guidance of Executive Director of that business. Once the business decisions are made, input into the planning process and how to manage data and protect privacy involves managers from all relevant teams.

**All staff**: Everyone who works with EMPHN in teams which hold personal information in hard copy, must ensure paper files are kept in a secure environment. Access is strictly controlled by the teams that have collected the information. The manager of that area acts as the Data Custodian and ensures access is closely monitored and limited to individuals whose role it is to action that information for the purpose it was collected.

## Where to get help?

- For enquires about this Privacy Policy, contact the policy owner: the Privacy Officer and Chief Operating Officer)
- Complete the feedback form on our website or intranet to let us know if you have any suggestions for how this policy could be improved, want to make a complaint, or even tell us what you like about this or any of our policies.

## Related EMPHN policies & procedures

- Feedback & Complaints Policy
- Information Security Policy
- ITC User Access Policy
- Third-party ITC User Access Policy
- Data Breach Response Plan
- Risk Management Framework
- Code of Conduct
- Employee contracts
- Provider contracts
- Procurement Policy
- Clinical Governance Framework
- SupportConnect Clinical Governance Policy

## References


- oaic.gov.au/privacy/australian-privacy-principles-guidelines
- National Statement on Ethical Conduct in Human Research (2018)
- Ethical conduct in research with Aboriginal and Torres Strait Islander Peoples and Communities guidelines (NHMRC, 2018)
- The Guidelines for Ethical Research in Australian Indigenous Studies (AIATSIS, 2012 [2020 edition forthcoming])
- The Guidelines for the Ethical Conduct of Evaluations (AES, 2013)