Privacy Policy

Purpose of this policy

EMPHN collects and holds information from individuals and organisations. We use that information to develop and support programs to 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, and how we protect individuals' personal information.

Scope of this policy

The policy covers privacy protections for:

- 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 EMPHN collects and holds from employees, Board, committee and advisory body members

Privacy protection at EMPHN extends to datasets holding deidentified consumer and clinical information.

Everyone who works for and with EMPHN must treat personal information ethically – respecting individuals' privacy and confidentiality, and take all reasonable steps to protect it.

Privacy protections and guiding principles

Privacy at EMPHN is protected by adherence to the Australian Privacy Principles, the Privacy Act (1988), and the Privacy and Other Legislation Amendment Act (2024); plus significant organisational and technological controls that have been put in place aligned with the ISO27001 Information Security Management System (ISMS). Owing to the higher standards afforded to the sensitive and health information of health consumers, this policy is also aligned with the Commonwealth and Victorian Health Records Acts, and the Victorian Privacy and Data Protection Act.

Guiding principles:

- Prior to collecting personal health information, we seek consent; and clearly 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
- Sharing or disclosing personal health information is directly aligned to the consent received
- 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
- Disclosures of identifiable personal health information not consented to are made according to 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
- Profile information – information and data with personal identifiable features (such as name, address and Medicare number) removed
- De-identified information – information and data with all identifiable features removed, then aggregated, scrambled and encrypted to ensure risks of reidentification are mitigated

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.

Profile information
EMPHN and EMPHN funded providers also share some personal health information from health consumers such as age, gender and postcode (but not name, address or Medicare number) with the Federal and Victorian Departments of Health to better understand a health service's reach and performance and its value to the community. Consent is sought to collect and share this information. If consumers do not consent, their use of the service is still reported – without their profile information such as age or gender.

Deidentified health information
EMPHN collects de-identified data from its funded health services that is aggregated 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. De-identification is done to a level that significantly minimises or eliminates the risk of re-identification, and then the data is further scrambled and encrypted. This aggregated, 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. Consent is sought to collect and share this information. For secondary uses such as research where it is not possible to go back to consumers to seek consent, EMPHN will ensure that privacy considerations are forefront and that research is aligned with the appropriate ethics framework.

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

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 and Complaints 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 Disability and Ageing, 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 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 services get from consumers to provide health services. (*To access an EMPHN-funded service 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, Disability and Aging, and the Victorian 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 collect and share relevant information** with other services, carers and supports relevant to assist the consumer's overall provision of care – helps EMPHN and service providers offer high-quality, safe care for consumers
4. **Consent to collect information for program evaluation** to support continual improvement of EMPHN-funded services.

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, with these exceptions: where:
    - the immediate safety of the consumer is at risk
    - public health considerations override normal consent rules
    - a consumer is identified as missing – EMPHN may provide contact details to the official locating entity (such as the Police)
- 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 seeks additional consent from the general practice if that de-identified data is subsequently used 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 certain (eg emergencies) circumstances, EMPHN may be required to share personal information by either state or federal legislation

Research and program evaluation – privacy considerations

EMPHN-funded health programs require consent from consumers to collect, use and disclose personal information before the service is delivered. Data from these sessions of service is aggregated to create deidentified datasets EMPHN uses to inform program improvement.

The de-identified personal information in EMPHN's datasets is maintained with a high standard of security that eliminates or significantly reduces the possibility that data can be re-identified at any point, with additional organisational and technological protections in place. For datasets with single linkage keys (SLKs) assigned, access for analysis, evaluation or research is tightly controlled once de-identification, data scrambling and encryption have been implemented.

While in a perfect world, the best option is to ask for explicit consent for all the purposes the data is to be used for – at the point of collection – that may not always be possible. Although research projects and evaluations (that go beyond program improvement) may benefit from accessing EMPHN's datasets, it's essential that disclosing information for research is always done in light of the need to protect sensitive, personal information.

Where it is not possible to get consumer consent to use deidentified datasets for research, EMPHN ensures research requests are vetted and managed according to Section 95A of the Privacy Act 1988, and the National Health and Medical Research Council's National Statement on Ethical Conduct in Human Research 2023.

NOTE: Research must also comply with the Ethical conduct in research with Aboriginal and Torres Strait Islander Peoples and Communities guidelines (NHMRC, 2018) to protect community members who participate in the research, and where the research is specifically about the Aboriginal and or Torres Strait Community, the AIATSIS Code of Ethics for Aboriginal and Torres Strait Islander Research (AIATSIS 2020) must be applied.

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 health information provided by clinics is de-identified before EMPHN receives it
- Data security is managed by the Data Analytics team, and overseen by the Information Management and Data Governance Committee according to the Information Governance and Management 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.
- Where there is no consent to disclose, 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 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 also provide privacy 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 and the Information Security Policy.

How we manage breaches

If there is a breach in EMPHN's information systems and personal information is at risk, we follow our established Cyber Incident Response Plan to immediately stop the access or distribution, and protect the rest of the information we hold. At that point, we evaluate whether the 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.

Examples of serious harm include:

- identity theft or financial loss
- a likely risk of physical harm, such as by an abusive ex-partner
- serious psychological harm
- serious harm to an individual's reputation

If a data breach involving personal information likely to result in serious harm, the Privacy Officer works with the Executive Director of Engagement and Communications to contact the individuals impacted by the breach. The Privacy Officer also reports the breach to the Office of the Australian Information Commissioner according to the Notifiable Data Breaches scheme. If the My Health Record system is impacted, the Australian Digital Health Agency must also be notified.

While the organisation works to contain and minimise the likelihood of harm as a result of any breach, the Privacy Officer must report notifiable breaches to OAIC within 30 days of being made aware of a suspected breach. Where possible, notifications are made within 72 hours of a suspected breach being discovered.

NOTE: when a data breach occurs, if it can be managed successfully, and is not likely to result in serious harm, EMPHN does not report the breach to the individuals or OAIC.

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 timeframe.

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

Roles & responsibilities within this policy

Privacy Officer: The Privacy Officer has responsibility to notify the Office of the Australian Information Commissioner (OAIC) where a data breach of personal information held by EMPHN is likely to result in serious harm. The Privacy Officer also works with the Executive Director of Engagement and Communications to contact the individuals impacted by the breach.

Information Management and Data Governance Committee: the IMDG Committee oversees decisions on what data to collect, and how that data will be stored, used and shared.

Executive Director, Corporate Services: Testing our privacy protections, including technological and organisational controls is triggered and overseen by the Executive Director, Corporate Services. Serious breaches must undergo a full review by the ED, CS to ensure gaps are identified and improvements are implemented.

Managers: Access to personal information is strictly controlled. Managers of datasets, information systems and technology must ensure access is limited to individuals whose role it is to action that information for the purpose it was collected. Access permissions must be reviewed regularly to ensure staff changing roles or leaving the organisation have their access rights revoked prior to exiting the team or organisation.

All staff: Everyone who works with EMPHN must read and comply with this policy and the wider policy suite to ensure personal information is protected and privacy is upheld. Suspected breaches of privacy must be reported to a manager as soon as possible and logged in EMPHN's incident management system, TICKIT. Teams which hold personal information in hard copy, must ensure paper files are never left unattended while in use, and are kept in a secure, locked environment at all other times.

Breaches

Violations of this policy will result in disciplinary actions, such as loss of access to EMPHN's information systems or technology, or termination of employment or contracts.

Policy review

This policy is monitored according to the Policy Framework and the Policy Directory. It is reviewed every three years, or sooner as triggered by legislative or organisational change.

Related EMPHN policies & procedures

- Feedback & Complaints Policy
- Information Security Policy
- Third-party Information Security Policy
- Cyber Incident Response Plan
- Risk Management Framework
- Code of Conduct
- Acceptable Use of Information Systems and Technology Policy
- Procurement Policy
- Clinical Governance Framework
- SupportConnect Clinical Governance Policy
- SupportConnect Open Disclosure Policy
- Employee contracts
- Provider contracts

Guidelines and Standards

- oaic.gov.au/privacy/australian-privacy-principles-guidelines
- National Statement on Ethical Conduct in Human Research (2023)
- Ethical conduct in research with Aboriginal and Torres Strait Islander Peoples and Communities guidelines (NHMRC, 2018)
- The AIATSIS Code of Ethics for Aboriginal and Torres Strait Islander Research (AIATSIS 2020)

Legislation

- Privacy Act 1988
- Privacy and Other Amendments Act 2024

Where to get help?

- For enquires about this Privacy Policy, contact its owner, the Privacy Officer privacyofficer@emphn.org.au
- Complete the feedback form on our website or intranet to let us know if you have 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.