Privacy Policy

Who is CheckUP and the Application of this Privacy Policy

1.1 CheckUP is a not-for-profit organisation dedicated to better health for people and communities who need it most. Through our current range of health programs and initiatives, CheckUP has an established footprint in over 150 communities across Queensland and the Northern Territory.

1.2 We provide members with strategic leadership and dynamic sector-wide linkages. We support the work of government and non-government primary healthcare providers and agencies. We provide government and other stakeholders with an effective channel for comprehensive sector-wide consultation and communication.

1.3 CheckUP is governed by the Australian Privacy Principles ("APPs") under the Privacy Act 1988 ('the Privacy Act'). The APPs set out the way organisations and government agencies can collect and use, disclose and provide access to personal and sensitive information.

1.4 Personal information is information that identifies or could identify a person, whether it is true or not. It includes, for example, name, age, gender and contact details.

1.5 Sensitive information as defined by the Privacy Act 1988 (as amended) is also personal information but relates to an individual's opinions, views, racial or ethnic origin, political options or affiliations, religious beliefs, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices or criminal record or health, genetic, biometric information or biometric templates.

1.6 This document sets out CheckUP's Privacy Policy.

1.7 Notwithstanding any references to specific examples in this Privacy Policy, these examples are not to be taken as an exhaustive list of personal information collected by CheckUP which is subject to change from time to time.

2 Related documents

- Privacy Act 1988 (Cth)
- Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)
- CheckUP Health Information Management Procedure (O110)
- CheckUP Data Breach Response Plan (O111) DEFINITIONS

3 Definitions

3.1 Consent

Express – Express Consent is given explicitly, either orally or in writing. This could include a handwritten signature or an oral statement to signify agreement.

Implied – Implied consent arises where consent may reasonably be assumed from the circumstances and from the conduct of the individual.

3.2 Data Breach

When personal information held by an organisation is lost or subjected to unauthorised access, use, modification, disclosure, or other misuse. Examples include malicious breach of security e.g. cyber security incident; accidental loss of IT equipment or hard copy documents; negligent or improper disclosure of information such as sending it to the wrong postal address or email.

All known or suspected data breaches are recorded in the *CheckUP Data Breach Register (under development),* in accordance with the *CheckUP Data Breach Response Plan (O111) (under review).*

3.2.1 Eligible Data Breach Notification

Under the Privacy Amendment (Notifiable Data Breaches) Act 2017 notification of data breaches is required in certain circumstances.

An eligible data breach happens if:

(a) both of the following conditions are satisfied:

- there is unauthorised access to, or unauthorised disclosure of, personal information held by CheckUP and
- a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates; or

(b) the information is lost in circumstances where:

- unauthorised access to, or unauthorised disclosure of, the information is likely to occur; and
- assuming that unauthorised access to, or unauthorised disclosure of, the information were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates.

3.2.2 Remedial Action – Exception

If there has been a breach but CheckUP has taken steps to remove the effect of the breach before harm occurs (e.g. a lost device can be remotely wiped), then the breach need not be notified.

3.2.3 Serious Harm

CheckUP will consider the following issues to determine whether the likely consequences for individuals would constitute serious harm:

- The kind of information and its sensitivity;
- Whether the information is protected by any security measures and, if so, the likelihood that any of these security measures could be overcome;
- The person or kinds of persons who have obtained, or could obtain, the information;

- If the information received by unauthorised recipients was encrypted or another similar security technology was utilised to make the information meaningless the likelihood that those recipients would have, or could obtain, information required to circumvent the security and have, or are likely to have, the intention to cause harm;
- The nature of the harm;
- Any other relevant matters.

Examples of serious harm could include:

- Unauthorised disclosure of credit card details which could be used fraudulently
- Unauthorised loss or disclosure of health records which can adversely impact upon the mental health and reputation of an individual or family court proceedings.
- Serious physical. psychological, emotional, economic, and financial harm.

3.3 Disclosure

Personal information is disclosed to an external person or entity if:

- That person/entity does not already know the personal information and is not in a position to otherwise find it out; and
- The personal information is provided to the person/entity or placed in a position to enable them to find it out; and
- CheckUP ceases to have control over the external person/entity in relation to who will know the personal information in the future.

3.4 Health Information

Health information is generally information about someone's health. In particular, it is:

- Personal information or an opinion (e.g. a medical opinion) that is personal information and is about the health or a disability at any time of an individual, about an individual's expressed wishes about the future provision of health services to him or her (e.g. a desire not to be kept on a life support machine) or about a health service provided, or to be provided, to an individual (e.g.

administrative information relating to an admission and discharge dates and fees);

- Other personal information collected to provide, or in providing a health service;
- Other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs, or body substances; or
- Genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.

3.5 Identifier

An identifier of an individual is a number, letter or symbol, or a combination of any or all of those things, that is used to identify the individual or to verify their identity. This includes the individual's name, ABN or anything else prescribed by regulation.

3.6 Individual

A natural living person.

3.7 Personal Information

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.

3.8 Pseudonymity

Bearing or using a fictitious name.

3.9 Sensitive Information

Information or an opinion:

- About an individual's racial or ethnic origin; political opinions; membership of a political association; religious beliefs or affiliations; philosophical beliefs; membership of a professional or trade association or trade union; sexual preferences or practices; or criminal record, that is also personal information;
- Health information about an individual; or
- Genetic information about an individual that is not otherwise health information;
- Biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
- Biometric templates

4 Collection and use of personal information

CheckUP may collect personal information about an individual for the following reasons:

- To provide high quality health services for clients
- because an individual has provided it directly to CheckUP, for instance contact details, date of birth, gender and bank account details;
- to provide a service that they have requested, such as health services or providing details to their professional association for the allocation of continuing professional development points;
- to process their CheckUP membership;
- to provide members with the most appropriate services for their needs;
- to improve our services, for instance, through the collection and analysis of statistical and research data and the use of cookies;
- because they work for us;
- for purposes directly related to any of the above and any of CheckUP's services;
- providing follow-up on information regarding CheckUP including responding to comments or questions;
- to meet any requirements of government funding for programs including receiving, collecting, collating statistical information and reporting that may at times include personal or sensitive information;
- to monitor and evaluate existing services and plan for future services.

CheckUP only uses personal and sensitive information for purposes that are directly related to the reason individuals provided us with the information in the first place and where they would reasonably expect us to use their information. We may also use their personal information where required by law or for contract compliance and reporting purposes.

5 How we collect information

When possible, at the time personal and/or sensitive information is collected, CheckUP will provide individuals with information indicating why the information is required, what will be done with the information, to whom if anyone the information will be disclosed, and the reason for disclosure if disclosure is required.

Whenever possible, CheckUP will collect personal information directly from the individual unless unreasonable or impractical for us to do so.

CheckUP may collect personal information in a variety of ways, including when individuals:

- use CheckUP's services;
- use CheckUP's website;
- phone CheckUP;
- write to CheckUP;
- email CheckUP;
- visit CheckUP in person or at events;
- through interviews;
- forms and questionnaires; and
- other evaluations.

When CheckUP collects an individual's information, or as soon as practicable after, we will take reasonable steps to inform the individual:

- that the information has been received by CheckUP;
- how to contact CheckUP;
- if CheckUP has received their information from another source, the details of the information received and why it was received;
- why CheckUP is collecting the information;

- the consequences (if any) for the individual if they do not provide all or part of the information requested;
- the organisations or types of organisations to which CheckUP may pass the individuals information on to and the reason/s it is being passed to another organisation;
- that the individual can access and seek to correct their information;
- how complaints relating to their information can be made and how they will be handled; and
- whether CheckUP is likely to disclose information to overseas parties and if so, the countries in which those parties are located.

6 Disclosure of personal information

6.1 Disclosure of personal information to third parties

CheckUP will not disclose an individual's personal information to another person unless the individual has given consent or if one of the exceptions under the Privacy Act 1988 or other legislation or laws require or allow CheckUP to do so.

Specific rules exist for the disclosure of health information and further information on these can be found in the CheckUP Health Information Management Policy and Procedure.

Where possible, the information that could reasonably identify someone as an individual is first removed.

6.2 Exceptions

Except as set out above, CheckUP will not disclose an individual's information to a third party unless one of the following applies:

- The individual has given their consent for CheckUP to do so;
- The individual would reasonably expect us to use or give that information for another purpose related to the purpose for which it was collected (or in the case of sensitive information, it is directly related to the purpose for which it was collected);
- it is otherwise required or authorised by law;
- it will prevent or lessen a serious threat to somebody's life, health or safety or to public health or safety;

- it is reasonably necessary for us to take appropriate action in relation to suspected unlawful activity, or misconduct of a serious nature that relates to our functions or activities; or
- it is reasonably necessary for the enforcement of a law conducted by an enforcement body.

6.3 Examples of disclosure:

6.3.1 Ongoing quality care

Consumers of a health service may require care from other health services or health providers. To ensure quality care CheckUP will disclose necessary and relevant personal information to these other providers as part of the referral process. Consent will be obtained to make such referrals.

6.3.2 Contractual requirements

To deliver services, CheckUP seeks funding from other organisations to provide the services. This funding is provided with contractual obligations that require CheckUP to report on the use of the funding.

Generally, CheckUP will use de-identified information including number of patients seen on a visit and number of Aboriginal and Torres Strait Islander patients seen on a visit to be used for funding reporting purposes.

However, information required for reporting may at times contain personal information. In this instance, CheckUP will implement processes to inform patients of this requirement and gain their consent, as required under the Privacy Act 1988. Contractual obligations cannot breach the Privacy Act 1988 and all the processes in this policy and under the Act will be followed to ensure privacy of information is maintained as required.

6.3.3 CheckUP Database

CheckUP maintains a database of individual and service provider contact details as outlined in Sections 1.3, 1.4 and 3.1 of this policy. Contact details may be used to send information to providers participating in the Outreach programs, CheckUP electronic newsletters and other promotional materials to members and stakeholders and, also

Public Health alerts on behalf of Queensland Health to General Practitioners and Health Services. All CheckUP electronic newsletters, promotional material, and public health alerts include an option for recipients to unsubscribe, as outlined in Section 10 of this policy.

6.3.4 Events

When an individual signs up for any of CheckUP's events, CheckUP may release a copy of the delegates list for the event to event sponsors for the purpose of further promotion. Delegates will be given the option to withhold their consent to have their details disclosed in this manner at any time and as set out in this Privacy Policy.

6.3.5 Operational reasons

CheckUP may use personal information for management purposes, funding or monitoring of services, which is permitted under the Privacy Act 1988. The information used for these purposes is generally de-identified but when required some personal information may need to be used.

7 Disclosure of information overseas

CheckUP will not send personal information out of Australia without the consent of the individual. A signed and verified consent form must be obtained if the individual/organisation or their legal entity is able to provide consent. Where this is not practicable i.e., the consumer is incapable of giving consent, then the information can be sent if the request is verified.

At times, CheckUP may send un-identifiable data overseas for business or quality purposes, however, all information will have personal data removed.

8 Anonymity and pseudonymity

It is the individual's choice to provide information to CheckUP. Wherever it is lawful and practicable, individuals have the option not to identify themselves or to use a fictional name when interacting with us.

An individual can remain anonymous when using some parts of the CheckUP website or sites administered by CheckUP.

It may be necessary for CheckUP to collect an individual's personal or sensitive information if they would like certain materials or services. If they choose to withhold the information CheckUP requires, we may not be able to provide them the services they have requested.

The impact of choosing not to provide necessary information will be explained to the individual.

9 Information security

CheckUP takes appropriate steps to protect an individual's personal and sensitive information held by us from misuse, interference, unauthorised access, modification, loss or disclosure. This includes during use, storage, collection, processing and transfer, and destruction of the information.

The CheckUP website may contain links to external websites. We recommend that individuals review the privacy policies of those external websites as CheckUP is not responsible for their privacy practices.

10 How to access and correct information

CheckUP will take reasonable steps to ensure that all personal information collected, used or disclosed is accurate, up-to-date, complete, relevant, and not misleading.

CheckUP will correct any personal information believed to be incorrect, out-of-date, incomplete, irrelevant or misleading. This may include taking reasonable steps to notify any organisation or government agency to which information was disclosed about the correction.

An individual may request to access or correct their personal information at any time by contacting the Privacy Officer. CheckUP will give an individual access to their information unless one of the exceptions under the Privacy Act 1988 applies. For example, if providing access would be unlawful or denying access is authorised by law.

If an individual requests access or to correct their information, CheckUP will respond within a reasonable time (usually within 30 days). If the request is refused, CheckUP will provide a written notice that sets out the reasons for refusal and how to complain about the decision.

11 Direct communications and promotional materials

From time to time, CheckUP may send out promotional materials for marketing purposes.

An individual's details collected for the purposes of providing a health service will not be used for the purposes of direct marketing communications or promotional materials.

If individuals do not wish to receive these communications, they can notify CheckUP to unsubscribe from that mailing list.

An individual's information may also be used by CheckUP to provide them with details of other organisation's services where permitted by the Privacy Act 1988 or where the individuals have consented to the use or disclosure of their personal information for direct communications and promotional materials.

It is CheckUP's policy that any direct communications or promotional material will include a statement advising that if an individual can request not to receive further material by contacting us using the details provided.

12 Cookies

The CheckUP website and sites administered by CheckUP uses software known as 'cookies' to record individuals who visit the website and collect some statistical information. CheckUP uses this information to help administer and improve our websites. We do not use this information to personally identify individuals. Information we may collect includes:

- The individual's server address
- The individual's domain name
- the date and time or access to the website
- pages accessed and documents downloaded
- the previous site visited
- if the individual has visited the website before
- the type of browser software in use.
- A person may set their browser to disable cookies when visiting CheckUP websites. However, some website functions may be unavailable if Cookies are disabled.

13 Complaints and enquiries

CheckUP is committed to the protection of individual's privacy. Questions about how CheckUP handles personal information, how to make a complaint about CheckUP's handling of someone's information, notification of a suspected data breach or the need for further information about the Privacy Policy, should be directed to the Privacy Officer. The Privacy Officer will assess any complaints and liaise with the individual to resolve any issues within a reasonable time (usually within 30 days).

14 Notification of eligible data breach

All data breaches will be assessed by CheckUP to determine if there are reasonable grounds to believe that the circumstances of the breach amount to an eligible data breach. If there has been a breach but CheckUP has been able to take steps to remove the effect of the breach before harm occurs (e.g. a lost device can be remotely wiped), then the breach will not be notified.

If CheckUP believes that there has been an eligible data breach then CheckUP will:

- Prepare a statement that complies with the Privacy Act: and
- Give a copy of the statement to the Office of the Australian Information Commissioner.

The statement will include:

- CheckUP's identity and contact details
- A description of the eligible data beach that CheckUP has reasonable grounds to believe has occurred
- The type of information concerned with the breach
- Recommendations about the steps that individuals should take in response to the eligible data breach
- If the breach involves other organisations the identity of those organisations.

If practical, CheckUP will notify the content of the statement to each of the individuals to whom the relevant information relates to and/or individuals who are at risk from the eligible data breach. If this is not possible CheckUP will publish a copy of the statement on its website and take any other reasonable steps to publicise the information.

15 Updating the Privacy Policy

CheckUP will update its Privacy Policy at least every two years or as required. The website will have the most current Privacy Policy www.checkup.org.au. The CheckUP Health Information Management Procedure (O110) is to be reviewed in line with this Privacy Policy and any relevant amendments be documented concurrently, to ensure consistency.

Changes to this Privacy Policy are communicated to CheckUP staff through staff meetings and staff are educated frequently on the requirements set out in this policy during these meetings. Health service providers are required to familiarise themselves with the CheckUP Privacy Policy each year during the contracting phase and other contractors and suppliers are advised of CheckUP's Privacy Policy upon commencements. Changes to the Policy are communicated through electronic newsletters.