2.5 PRIVACY and CONFIDENTIALITY

2.5.1 Policy

BPCC & BPPCC is committed to protecting the privacy of information collected and handled for the purposes of providing clinical or patient services.

BPCC & BPPCC handles all personal and health information in accordance with the *Privacy & Data Protection Act 2014*, *Health Records Act 2001* and complies with Federal and Victorian privacy regulations set out in the *Privacy Act 1988* and *Privacy Amendment (Enhancing Privacy Protection) Act 2012* as well as complying with standards set out in the *RACGP Handbook for the management of health information in general practice (3rd edition).*

All information and data collected by BPCC & BPPCC is deemed to be private and confidential and is held, used and disclosed in accordance with the *Privacy Act 1988*. All staff, contractors, volunteers and students are responsible for maintaining the privacy, confidentiality and security of personal and health information held by BPCC & BPPCC and are required to do so under the *Health Services Act 1988* and the *Mental Health Act 2014 (Vic*). All staff, contractors, volunteers and students are required to comply with the Health Privacy Principles (HPP) detailed in the *Health Records Act 2001* (See resources for link) and the Information Privacy Principles (IPP) contained in schedule 1 to the *Privacy and Data Protection Act 2014* (See resources for link). Significant breaches of confidentiality may provide grounds for disciplinary action or dismissal and may incur other legal consequences.

Under no circumstances are members of the practice team to discuss, disclose or in any way reveal patient conditions or documentation or personal details of colleagues to unauthorised staff, other colleagues, other patients, family or friends, whether at the practice or outside it, such as in the home or at social occasions without the patient's express consent. This includes patient's accounts, referral letters or other clinical documentation. The exception to this is if legislation or a court order requires disclosure, for example child protection, notifiable diseases, reporting death to a coroner, reporting a birth or death to the Register of Births, Deaths and Marriages, or a search warrant, subpoena or coroners request. *NB: Legislation does not generally permit disclosure to Police.*

According to the *Privacy Act 1988* and the *Australian Privacy Principles*, an organisation may use or disclose personal health information for a purpose (the secondary purpose) which is directly related to the primary purpose of collection without seeking consent, assuming that there is a reasonable expectation that this information could be used or disclosed for that secondary purpose. Examples of secondary purpose disclosures include but are not limited to management, funding and monitoring, complaint-handling, planning, evaluation and accreditation activities.

BPCC & BPPCC Staff members, including clinical staff, must only access a patients electronic health record where it is necessary to provide a service to them, to charge or make a claim for a service provided to them, to plan or allocate a service to them, to audit the record or evaluate a service or program. Staff members must not access their own files/records or that of family members or friends at any time.

2.5.2 Definitions

Privacy:	refers to the fundamental right that an individual has to keep their personal life or personal information secret and to control the flow of their personal information, including the collection, use and disclosure of that information.
Confidentiality:	refers to the secrecy and privileged status of an individuals personal information.

Personal Information:	is information or opinion about an individual who may be identified either directly or indirectly by that material. It can be any medium including written, verbal or electronic records, video or audio recordings, photographs, or labels on pathology samples etc. Personal information encompasses health information.
Health Information:	is information or opinion about an individuals physical, mental or psychological health or disability, expressed wishes about provision of future health services or other personal information collected by any individual for or on behalf of BPCC & BPPCC in order to provide a health service.
Employee Record:	a record of personal information relating to the employment of the individual, including but not limited to: • The terms and conditions of employment, ie hours of work, salary/wages, emergency contact details, personal information, credentials • The engagement or training of the employee • The employees performance or conduct • The disciplining, resignation or termination of the employee • The employees OH&S or workcover discussions, history or records if applicable • Membership of a professional or trade association • Leave entitlements • Taxation, superannuation or banking details.
Disclosure:	Means to reveal any personal or health information to any person not directly involved in the individuals care or employment, including family, friends or staff in any form, ie verbally, in writing or by copying it either at the practice or outside it, during or outside normal opening hours, except for strictly authorised use within the patient care context at the practice or as legally directed.
Misconduct:	Is defined as unsatisfactory behaviour by means of an intentional or negligent failure to abide by or adhere to the standards of conduct expected
Serious Misconduct:	As described under the Fair Work Regulations 2009 is conduct that includes both of the following: (a) Wilful or deliberate behaviour by a staff member that is inconsistent with the continuation of the contract of employment; (b) Conduct that causes serious and imminent risk to: (i) The health and safety of a person; or (ii) The reputation, viability or profitability of the employers business.

2.5.3 Purpose

To ensure that all staff members, including employees, contractors, volunteers and students are aware of their rights and responsibilities in relation to protecting the privacy of all BPCC & BPPCC patients and other staff.
To maintain a process by which breaches of this policy are dealt with in a consistent, appropriate and timely manner.

2.5.4 Procedure

All members of the practice team are issued with the practice's Privacy Policy Statement (see Appendix 1) and sign a *Privacy Statement* as part of their terms and conditions of employment or contract. The policies and procedures of the practice are further explained during the induction of new practice team members, and the induction form is signed by the new team member as confirmation that they understand and accept their obligations in relation to patient privacy and the confidentiality of personal health information.

Our privacy policy statement is displayed in the waiting room and also on the practice information sheet and practice website, and is readily presented to anyone who asks.

Patient consent for the transfer of health information to other providers or agencies involved in their healthcare (e.g. treating practitioners and specialists outside the practice) is obtained at the patient's first visit to our practice through the *New Patient Information Form*. Once signed, this form is scanned into the patient's health record and its completion is noted.

Prior to a patient signing consent to the release of their health information, patients are made aware they can request a full copy of our privacy policy.

Patients of BPCC & BPPCC are also advised of 'secondary purpose' disclosures. This is done in a number of ways, including:
At the time of the consultation with a general practitioner
Via the practice privacy statement in the practice information sheet
Via the practice privacy statement on signage on the walls of the practice, and/or
By reading, understanding and signing a new patient information form when first registering at the practice, which incorporates the practice privacy statement.

Patients have the right to 'opt out' of the secondary purpose through refusal to consent and their non-consent is recorded on their file.

There are also privacy risks associated with any form of communication in that the information could be intercepted, read or overheard by someone other than the intended recipient. Our patients' health records are solely electronic, therefore our practice is considered paperless and has systems in place to protect the privacy, security, quality and integrity of the personal health information held electronically. Appropriate staff members are trained in computer security policies and procedures.

- **Email** communications with other healthcare providers is undertaken securely through the use of encryption. Email communication with patients is discouraged; however, where initiated by the patient, the risks are communicated and patient consent is obtained.
- Where patient information is sent by **post**, the use of secure postage or a courier service is determined on a case by case basis.
- Incoming patient correspondence and diagnostic **results** are opened and viewed only by a designated practice team member.
- Items for collection or postage are left in a secure area not in view of the public.
- **Facsimile, printers and other electronic communication** devices in the practice are located in areas that are only accessible to the general practitioners and other authorised team members. Faxing is point to point and will, therefore, usually only be transmitted to one location. All facsimiles containing confidential information are sent only after ensuring the facsimile number dialled is the designated receiver before pressing 'Send'. Details of confidential information sent by facsimile are recorded in a designated logbook which incorporates the date of transmission, patient name, description of the contents and the designated receiver (name and facsimile number). A copy of the transmission report produced by the facsimile is kept as evidence that the facsimile was successfully transmitted, and as evidence the information was sent to the correct facsimile number. Facsimiles received are managed according to incoming correspondence protocols. The words 'Confidential' are to be recorded on the header of the facsimile coversheet and a facsimile disclaimer notice at the bottom of all outgoing facsimiles affiliated with the practice.

IMPORTANT: THIS FACSIMILE TOGETHER WITH ANY ATTACHMENTS IS INTENDED FOR THE ADDRESSEE ONLY AND MAY CONTAIN CONFIDENTIAL OR PRIVILEGED INFORMATION. IF YOU ARE NOT THE INTENDED RECIPIENT, YOU ARE NOTIFIED THAT ANY USE OR DISSEMINATION OF THIS COMMUNICATION IS STRICTLY PROHIBITED. IF YOU HAVE RECEIVED THIS COMMUNICATION IN ERROR, PLEASE NOTIFY THE SENDER AT THE ABOVE ADDRESS IMMEDIATELY AND DESTROY ALL COPIES OF THIS TRANSMISSION TOGETHER WITH ANY ATTACHMENTS

- Patient privacy and security of information is maximised during consultations by closing the consulting room doors. When the consulting, treatment room or administration office doors are closed, practice team members must ensure they knock and wait for a response prior to entering.
- Where locks are present on individual rooms, these should not be engaged except when the room is not in use.
- It is the general practitioner/healthcare team member's responsibility to ensure that prescription paper, patient health records and related personal information is kept secure if they leave their room during a consultation or treatment, or whenever they are not in attendance in the consulting/treatment room.
- The physical health records and related information created and maintained for the continuing management of each patient are the property of this practice. This information is deemed a personal health record and while the patient does not have ownership of the record, he/she has the right to access under the provisions of the *Privacy Act 1988*. Requests for access to a patient's health record will be acted upon only if the request is received in written format.
- Both active and inactive patient health records are kept and stored securely.
- Members of the practice team have different levels of access to personal patient health information as appropriate to their roles and to maintain security all computer hardware and software passwords are kept confidential and are not disclosed to others (refer to **Section 6.2 - Computer information security**)

2.5.5 Breach Process

There are a number of scenarios that may constitute a privacy breach relating to inappropriate access to health information of a BPCC & BPPCC patient/client, where the person accessing the information does not have a direct clinical or business purpose to do so (see Appendix 2).

A breach of privacy may also constitute a breach of BPCC & BPPCCs Code of Conduct and/or the Privacy Act 1988 and may not only result in disciplinary action (including termination of employment), but may be considered an offence which attracts penalties under privacy legislation.

BPCC & BPPCC will investigate any and all suspected breaches of patient privacy.

Suspected breaches must be reported to the staff members line manager and/or General Manager using the 'Incident, Hazard, Injury Report form'. Reports should include the name/s of the staff member/s involved, full name & DOB of the patient, dates relating to the suspected breach and any other relevant information that is known.

All suspected breaches must be investigated. This involves an audit of the software systems to determine if and when the staff member has accessed the unauthorised information, and interviews of all people involved. The investigation will be facilitated by the staff members Line Manager and the General Manager and in some circumstances, may be referred to an external investigator. The staff member will be notified of the outcome of the investigation. All meetings with the staff member will be recorded and a copy given to the staff member.

If the investigation indicates a breach has occurred, the disciplinary process must be followed. This may be dependent on the type or breach, intent behind the breach and the harm/potential harm sustained as a result of the breach. The staff member will be notified of the action that will be taken. The staff member is entitled to bring a support person or union representative to this meeting

If the person is found guilty of misconduct, disciplinary action may include:

- Formal counselling,
- Reprimand by way of a formal warning.
- (Reassignment of duties
- Deduction in salary, by way of a fine
- Reduction in classification, which may result in a reduction in salary)

For serious misconduct, disciplinary action may include:

- Final formal warning
- Termination of employment.

Please see **2.7 Disciplinary action and termination process**

Resources/References

- Privacy Act 1988
- Privacy Amendment (Enhancing Privacy Protection) Act 2012
- Health Privacy Principles – https://www.health.vic.gov.au/rights-and-advocacy/rights-and-privacy-principles
- Information Privacy Principles https://ovic.vic.gov.au/privacy/information-privacy-principles-full-text/
- RACGP Handbook for the management of health information in general practice (3rd edition) available from https://www.racgp.org.au/download/Documents/e-health/handbook-for-the-management-of-health-information-in-general-practice-.pdf

3. RACGP Standards-for-general-practice-5th-edition https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/privacy-of-health-information/use-and-disclosure-of-health-information/privacy-policies

- Health Records Act 2001 (Vic)
- Privacy & Data Protection Act 2014
- Health Services Act 1988
- Mental Health Act 2014 (Vic)

Approval

Callum Wright, General Manager
Date: 05 March 2025

Appendix 1

BENDIGO
PRIMARY CARE
CENTRE

Privacy Statement

I, _____ understand BPCC's requirement to protect the privacy of information as detailed below.

All patient records including clinical data, accounts, verbal discussions, written documents including those emanating from computers or facsimile machines heard, written, received or otherwise produced by others or myself, are deemed strictly private and confidential and are not to be discussed or in any way released to anyone except under instruction by the General Manager or designate, and according to privacy law*.

This privacy statement is binding even if I am no longer employed by BPCC.

I understand and am aware of the confidentiality requirements and recognise that significant breaches of confidentiality may provide grounds for dismissal.

Signed: _____ Date: ___/___/_____

Declared before: _____ (Print full name of first witness in block letters)

Job title: _____

Signed by witness: _____ Date: ___/___/_____

* Commonwealth Privacy Act (1988) & its amendments

* Victorian Health Records Act (2001)

Document title: Privacy Statement Form
Reviewed by: Dr Steve Cooper / General Manager
Version : 1 Effective Date: 1st May 2020
Next Review Date: 1st May 2023

BPCC & BPPCC Privacy Policy Statement

Our practice privacy policy states:

"Your privacy is important to us. It is BPCC & BPPCC's policy to respect your privacy regarding any information we may collect from you across our website, www.bendigoprimarycarecentre.com.au, and other sites we own and operate. We only ask for personal information when we truly need it to provide a service to you. We collect it by fair and lawful means, with your knowledge and consent. We also let you know why we're collecting it and how it will be used. We only retain collected information for as long as necessary to provide you with your requested service. What data we store, we'll protect within commercially acceptable means to prevent loss and theft, as well as unauthorised access, disclosure, copying, use or modification. We don't share any personally identifying information publicly or with third-parties, except when required to by law. Our website may link to external sites that are not operated by us. Please be aware that we have no control over the content

and practices of these sites, and cannot accept responsibility or liability for their respective privacy policies. You are free to refuse our request for your personal information, with the understanding that we may be unable to provide you with some of your desired services. Your continued use of our website will be regarded as acceptance of our practices around privacy and personal information. This policy does not apply to personal information you provide to the BPCC & BPPCC in the course of using our services. Any personal information you provide as a patient is governed by the Health Records Act 2001 (Vic) and our privacy policy. If you have any questions about how we handle user data and personal information, feel free to contact us. This policy is effective as of 20 January 2020"

Appendix 2

Scenarios that may constitute a privacy breach may include, but are not limited to;

- Accessing/viewing your own health information
- Accessing/viewing a family members health information
- Accessing/viewing the record of another staff member or someone known to them
- Accessing/viewing the record of a high profile patient (ie something that has been reported in the media, well known person etc)