PATIENT PRIVACY POLICY

Introduction

This privacy policy is to provide information to you, our patient, on how your personal information (which includes your health information) is collected and used within our practice, and the circumstances in which we may share it with third parties. A personal health record is a collection of your personal health information.

Why and how your consent is necessary

When you register as a patient of our practice, you provide consent for our GPs and practice staff to access and use your personal information so they can provide you with the best possible healthcare. Only staff who need to see your personal information will have access to it. If we need to use your information for anything else, we will seek additional consent from you to do this.

Why do we collect, use, hold and share your personal information

Our practice will need to collect your personal information to facilitate the provision of healthcare services to you by the independent medical practitioners operating from our practice. Our main purpose for collecting, using, holding and sharing your personal information is to facilitate the management of your health by those independent medical practitioners. We also use it for directly related business activities, such as financial claims and payments, practice audits and accreditation, and business processes (e.g. staff training).

What personal information do we collect

The information we will collect about you includes you're:

(a) Names, date of birth, addresses, contact details including emergency contact and next of kin.
(b) Demographic information, including gender, cultural background, and religious beliefs.

(c) Medical information including medical history, medications, allergies, adverse events, immunizations, social history, family history and risk factors.
(d) Medicare number (where available) for identification and claiming purposes.
(e) Healthcare identifiers;
(f) Payment and/or financial information.
(g) Concession card details; and
(h) Health fund details.

Dealing with us anonymously

You have the right to deal with us anonymously or under a pseudonym unless it is impracticable for us to do so or unless we are required or authorized by law to only deal with identified individuals.

Please be aware that Medicare rebates are only available where a Medicare card (and/or associated information) is available. As such your doctor may require you to pay for your consultations in full without this rebate if you choose to deal with us anonymously or under a pseudonym.

How do we collect your personal information

Our practice may collect your personal information in several different ways:
You may provide us with your personal information directly (for example, when you make an appointment with a medical practitioner operating from our practice, our practice staff will collect your personal and demographic information via your registration).

The medical practitioners providing medical services may also collect further personal information from you which may be disclosed to us. Information can also be collected through My Health Record, e.g., via Shared Health Summary, Event Summary or through a Discharge Summary provided by a hospital or other healthcare service providers.

We may also collect your personal information when you contact us via our website, send us an email or SMS, telephone us, make an online appointment or communicate with us using social media.

In some circumstances personal information may also be collected from other sources. Often this is because it is not practical or reasonable to collect it from you directly. This may include information from:

(i) Your guardian or responsible person.

(ii) Other involved healthcare providers, such as specialists, allied health professionals, hospitals, community health services and pathology and diagnostic imaging services; and/or
(iii) Our health fund, Medicare, or the Department of Veterans' Affairs (as necessary).

If a clinician deems it in your best interest to discuss your clinical information with you, we will arrange for this to occur either in person, via telephone or via videoconference.

When why and with whom do we use and share your personal information

We collect, use and disclose your personal information to provide medical services to patients of the general practitioners operating from our practice.

We may also share your personal information:

(a) With other healthcare providers.
(b) When it is required or authorized by law (e.g., court subpoenas, or where we are obliged to make a mandatory notification to a regulatory body);
(c) When it is necessary to lessen or prevent a serious threat to a patient's life, health or safety or public health or safety, or where it is otherwise impractical to obtain your consent.
(d) To assist in locating a missing person.
(e) To establish, exercise or defend a claim.
(f) For confidential dispute resolution processes.
(g) While providing nursing support services.
(h) For the purposes of uploading that information to your My Health Record, such as through the shared health summary or event summary; and/or
(i) With third parties who work with our practice for business purposes, such as accreditation agencies or information technology providers – these third parties are required to comply with the Australian Privacy Principles (APPs) and this policy.

Only people who need to access your information will be able to do so. Other than while facilitating the provision of medical services or as otherwise described in this policy, our practice will not share personal information with any third party without your consent.

We will not share your personal information with anyone outside Australia (unless under exceptional circumstances that are permitted by law) without your consent.

Our practice will not use your personal information for marketing any of our goods or services directly to you without your express consent. If you do consent, you may opt out of direct marketing at any time by notifying us of our practice in writing.

How do we store and protect your information?

Your personal information may be stored at our practice in various forms.

Our practice stores information as electronic records (including via cloud-based services), visual records (including photos) and archived paper records.

Our practice stores all personal information securely via passwords, encrypted back-ups, confidentiality agreements for staff, and secure cabinets.

All records will be retained until the later of seven (7) years from your last contact with the practice, or until you reach the age of twenty-five (25).

We take steps to destroy or de-identify information that we no longer require.

Our server security policy is designed to protect the servers from unauthorized access, data breaches, and other security threats. Our practice uses the following security measures to ensure the personal information which it holds is secured:

(a) Antivirus software is installed on all servers and updated regularly.
(b) Firewalls are configured to block unauthorized traffic.
(c) Servers are placed on their own subnet.
(d) Access to servers is restricted to authorized users.
(e) Physical access to the servers is limited, with servers located in a locked room and security cameras installed around the building.
(f) Servers are patched regularly to fix security vulnerabilities.
(g) Backups are created regularly every hour onsite with daily offsite backups.

How can you access and correct your personal information at our practice?

You have the right to request access to, and correction of, your personal information.

Our practice acknowledges patients may request access to their medical records. We require you to put this request in writing and send to the clinics mailing address. Alternatively, you can email your request to reception@jsnmedical.com.au and our practice will respond within 30 business days. Should JSN Medical comply with the request please note that a fee may be associated with providing this information.

Our practice will take reasonable steps to correct your personal information where the information is not accurate or up to date. Each time you visit, we will ask you to verify that your personal information held by our practice is correct and current. You

may also request that we correct or update your information, and you should make such requests in writing addressed to our reception team at reception@jsnmedical.com.au

How can you lodge a privacy-related complaint, and how will the complaint be handled at our practice?

We take complaints and concerns regarding privacy seriously. You should express any privacy concerns you may have in writing. We will then attempt to resolve it in accordance with our resolution procedure.

Complaints can be addressed to JSN Medical admin manager at admin@jsnmedical.com.au or via post to 501A Wiltshire Lane, Delacombe Victoria 3356 . The admin manager can also be contacted by telephone on (03) 4327 0755. Our admin manager has 30 business days to respond to your complaint.

You may also contact the Office of the Australian Information Commissioner (OAIC). Generally, the OAIC will require you to give them time to respond before they investigate. For further information, visit www.oaic.gov.au

Policy review statement

This privacy policy will be reviewed regularly to ensure it is in accordance with any changes that may occur. Amended policies will be available to patients as changes occur.

Review date 23/07/2024

****

INTERNET AND EMAIL POLICY

Introduction

JSN Medical recognises the practice team requires access to email and the internet to assist in the efficient and safe delivery of healthcare services to our patients.

Purpose and objectives

This policy sets out guidelines for acceptable use of internet and email by the practice team, contractors and other staff of JSN Medical. Internet and email is provided to assist the team carry out their duties of employment.

Scope

This internet and email policy applies to the practice team, contractors and other staff of JSN Medical who access the internet and email on practice owned devices including, but not limited, to the practice email accounts, internet and network access, laptops and desktop computers to perform their work.

Use of the internet by the practice team, contractors and other staff is permitted and encouraged where this supports the goals and objectives of JSN Medical. Access to the internet is a privilege and the practice team, contractors and other staff must adhere to this policy.

Violation of these policies could result in disciplinary action.

Actions could include

- disciplinary and/or legal action
- termination of employment

- the practice team, contractors and other staff being held personally liable for damages caused by any violations of this policy

All employees are required to confirm they have understood and agree to abide by this email and internet policy. A statement of this policy will be provided to each staff member who must sign, date, and agree to the terms of this policy.

Policy content

The practice team, contractors and other staff must only use the internet and email access provided by JSN Medical for:

- Work and work-related purposes

Unacceptable internet and email use

The practice team, contractors and other staff may not use internet or email access provided by JSN Medical to:

- Creating or exchanging messages that are offensive, harassing, obscene or threatening
- Visiting web sites containing objectionable (including pornographic) or criminal material
- Exchanging any confidential or sensitive information held by JSN Medical.
- Creating, storing, or exchanging information in violation of copyright laws
- Using internet-enabled activities such as gambling, gaming, conducting a business or conducting illegal activities
- Creating or exchanging advertisements, solicitations, chain letters and other unsolicited or bulk email
- Playing electronic or online games in work time

Policy review statement

This policy will be reviewed regularly to ensure it reflects the current processes and procedures of JSN Medical and current legislation requirements.

****

SOCIAL MEDIA POLICY

Introduction

This policy provides guidance for members of the practice on using social media internally and externally. The policy helps identify and mitigate risks associated with social media use.

Notion

‘Social media’ is online social networks used to disseminate information through online interaction.

Regardless of whether social media is used for business-related activity or for personal reasons, the following policy requirements apply to all GPs and practice staff of the practice. GPs and practice staff are legally responsible for their online activities, and if found to be in breach of this policy consequences may include disciplinary action or even termination of employment.

Use of practice social media accounts

The practice Admin team are responsible for managing and monitoring the practice’s social media accounts. All posts on the practice’s social media website must be approved by this team or by the Medical Director. The practice reserves the right to remove any content at its own discretion.

Staff conduct on social media

When using the practice’s social media, practice staff will not

- Post any material that:

  - is unlawful, threatening, defamatory, pornographic, inflammatory, menacing, or offensive
  - infringes or breaches another person's rights (including intellectual property rights) or privacy, or misuses the practices or another person's confidential information (e.g. do not submit confidential information relating to our patients, personal information of staff, or information concerning the practice's business operations that have not been made public)
  - is materially damaging or could be materially damaging to the practice's reputation or image, or another individual
  - is in breach of any of the practice's policies or procedures
- Use social media to send unsolicited commercial electronic messages, or solicit other users to buy or sell products or services or donate money
- Impersonate another person or entity (e.g. by pretending to be someone else or another practice employee or other participant when you submit a contribution to social media) or by using another's registration identifier without permission
- Tamper with, hinder the operation of, or make unauthorised changes to the social media sites
- Knowingly transmit any virus or other disabling feature to or via the practice's social media account, or use in any email to a third party, or the social media site
- Attempt to do or permit another person to do any of these things
  - claim or imply that you are speaking on the practice's behalf, unless you are authorised to do so
  - disclose any information that is confidential or proprietary to the practice, or to any third party that has disclosed information to the practice
- Be defamatory, harassing or in violation of any other applicable law
- Include confidential or copyrighted information (e.g. music, videos, text belonging to third parties)
- Violate any other applicable policy of the practice.

Monitoring social media sites

The practice's social media channels are part of our customer service and should be monitored and dealt with regularly. This will be done by the Medical Director and Admin team.

Our practice complies with AHPRA national law and takes reasonable steps to remove testimonials that advertise their health services (which may include comments about the practitioners themselves). The practice is not responsible for removing (or trying to have removed) unsolicited testimonials published on a third-party website or in social media accounts over which they do not have control.

Personal social media use

Staff are free to personally engage in social media outside of work hours, as long as their actions do not have the potential to bring the practice into disrepute. Employees may not represent personal views expressed as those of this practice.

Any social media posts by staff on their personal social media platforms must not reveal confidential information about the practice or a person who uses the practice (eg staff should not post information relating to patients or other staff, or information concerning the practice's business operations that have not been made public).

Staff should respect copyright, privacy, fair use, financial disclosure, and other applicable laws when publishing on social media platforms.

Breach of policy

All social media activities must be in line with this policy.

Policy review statement

This policy will be reviewed regularly to ensure it is up to date with changes in social media or relevant legislation

Current as of: 23/07/2024

****