iSpot Clinic Privacy Policy
Current from January 2019

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.

Why and when 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 provide healthcare services to you. Our main purpose for collecting, using, holding and sharing your personal information is to manage your health. We also use it for directly related business activities, such as financial claims and payments, practice audits and accreditation, and business processes (eg staff training).

What personal information do we collect?

The information we will collect about you includes:

- names, date of birth, addresses, contact details
- medical information including medical history, medications, allergies, adverse events, immunisations, social history, family history and risk factors
- Medicare number (where available) for identification and claiming purposes
- healthcare identifiers
- 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 authorised by law to only deal with identified individuals.

How do we collect your personal information?

Our practice will collect your personal information:

1. When you make your first appointment our practice staff will collect your personal and demographic information via your registration.
2. During the course of providing medical services, we may collect further personal information. For example the Electronic Transfer of Prescriptions (eTP) system. If you register for the MyHealth Record or PCEHR system your health information will be uploaded to that system.
3. We may also collect your personal information when you visit our website, send us an email, telephone us, make an online appointment or communicate with us using social media.
4. 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:

- your guardian or responsible person
- other involved healthcare providers, such as specialists, allied health professionals, hospitals, community health services and pathology and diagnostic imaging services
- your health fund, Medicare, or the Department of Veteran's Affairs.

Who do we share your personal information with?

We sometimes share your personal information:

- 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 APPs and this policy
- with other healthcare providers
- when it is required or authorised by law (eg court subpoenas)
- 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 it is impractical to obtain the patient's consent
- to assist in locating a missing person
- to establish, exercise or defend an equitable claim
- for the purpose of confidential dispute resolution process
- when there is a statutory requirement to share certain personal information (eg some diseases require mandatory notification)
- during the course of providing medical services, through Electronic Transfer of Prescriptions, MyHealth Record/PCEHR system.

Only people that need to access your information will be able to do so. Other than in the course of providing 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. None of our patient's health information is shared with any overseas agency or company.

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 our practice in writing. We usually notify our patients of recalls for clinical matters such as when a pap smear, colonoscopy or routine skin check occurs.

How do we store and protect your personal information?

Your personal information may be stored at our practice in various forms, but principally as an encrypted electronic file on a secure system. Paper records and letters are generally scanned, then shredded after a short holding period. Clinic photographs may be taken in consultations, but you will always be asked for your consent before such images are taken.

Our practice stores all personal information securely.

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 addressed to the Practice manager and our practice will respond within 30 days. Fees may be charged for accessing your health record. Access to read your health record attracts a fee of $15. To obtain a copy of some or all of your record the cost is $40 for the first 50 pages then 20c for each

page thereafter. A 50% discount applies to pensioners and DVA (Department of Veterans Affairs) patients on presentation of a relevant card (e.g. Pension Card, Health Care or Senior's Card holders). That is, $20 for the first 50 pages then 10c for every page thereafter. GST is not applicable.

Our practice takes reasonable steps to correct your personal information where the information is not accurate or up-to-date. From time-to-time, we will ask you to verify your personal information held by our practice is correct and up-to-date. You may also request that we correct or update your information, and you should make such requests in writing to Lisa Phare, Practice Manager.

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 addressed to Lisa Phare, Practice Manager. We will then attempt to resolve it in accordance with our resolution procedure. You must include your mailing address and contact number. We will endeavor to address any concerns you raise within 30 days of receipt.

You may also contact the OAIC. Generally the OAIC will require you to give them time to respond, before they will investigate. For further information visit www.oaic.gov.au or call the OAIC on 1300 336 002.

Privacy and our website / Facebook Page

Our website does not collect any personal information about you, unless you fill out one of the forms such as a repeat prescription form.

Facebook tells us if a patient has 'liked' or commented on our page.

Policy review statement

This policy will be reviewed annually and an updated copy uploaded to the clinic website.

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 and collection statement.

Patient consent for the transfer of health information to other providers or agencies is obtained on the first visit. A copy of our consent form is included below.

Once signed this form is scanned into the patient's record and its completion noted. Note: Consent for transfer of information differs from procedural consent.

6.2 3rd Party Requests for Access to Medical Records/Health Information

Policy

Requests for 3rd Party access to the medical record should be initiated by either receipt of correspondence from a solicitor or government agency or by the patient completing a Patient Request for Personal Health Information Form. Where a patient request form or and signed authorisation is not obtained the practice is not legally obliged to release.

Where requests for access are refused the patient or third party may seek access under relevant privacy laws.

An organisation 'holds' health information if it is in their possession or control. If you have received reports or other health information from another organisation such as a medical specialist, you are required to provide access in the same manner as for the records you create. If the specialist has written 'not to be disclosed to a third party' or 'confidential' on their report, this has no legal effect in relation to requests for access under the *Health Records Act 2001*. You are also required to provide access to records which have been transferred to you from another health service provider.

Requests for access to the medical record and associated financial details may be received from various 3rd Parties including:

1. Subpoena/court order/coroner/search warrant
2. Relatives/Friends/carers
3. External doctors & Health Care Institutions
4. Police /Solicitors
5. Health Insurance companies/Workers Compensation/Social Welfare agencies
6. Employers
7. Government Agencies
8. Accounts/Debt Collection
9. Students (Medical& Nursing)
10. Research /Quality Assurance Programs
11. Media
12. International
13. Disease registers
14. Telephone Calls

We only transfer or release patient information to a third party once the consent to share information has been signed and in specific cases informed patient consent has may be sought. Where possible de identified information is sent

Our practice team can describe the procedures for timely, authorised and secure transfer of patient health information in relation to valid requests.

Procedure

The practice team can describe how we correctly identify our patients using 3 patient identifiers, name, date of birth, address or gender to ascertain we have the correct patient record before entering, actioning or releasing anything from that record.

Patient consent for the transfer of health information to other providers or agencies is obtained on the first visit and retained on file in anticipation of when this may be required.

As a rule no patient information is to be released to a 3rd Party unless the request is made in writing and provides evidence of a signed authority to release the requested information, to either the patient directly or a third party. Where possible de identified data is released.

Written requests should be noted in the patient's medical record and also documented in the practice's Request Register. Requests should be forwarded to the designated person within the practice for follow-up.

Requested records are to be reviewed by the treating medical practitioner or principal doctor prior to their release to a third party. Where a report or medical record is documented for release to a third party, having satisfied criteria for release, (including the patients written consent and where appropriate written authorisation from the treating doctor), then the practice may specify a charge to be incurred by the patient or third party, to meet the cost of time spent preparing the report or photocopying the record.
Section 1.01
The practice retains a record of all requests for access to medical information including transfers to other medical practitioners.

Where hard copy medical records are sent to patients or 3rd Parties copies are forwarded not original documentation wherever possible. If originals are required copies are made in case of loss.

Security of any health information requested is maintained when transferring requested records and electronic data transmission of patient health information from our practice is in a secure format.

Subpoena, Court Order, Coroner Search Warrant

Note the date of court case and date request received in the medical record. Depending on whether a physical or electronic copy of the record is required follow procedures as described above. Refer also to section 8 "Management of potential Medical defence claims'

On occasions a member of staff is required to accompany the medical record to court or alternatively a secure courier service may be adequate. If the original is to be transported, ensure a copy is made in case of loss of the original during transport. Ensure that the record is returned after review by the court.
Relatives/Friends

A patient may authorise another person to be given access if they have the legal right and a signed authority. See 6.3 Patient Requests for Personal Health Information. See also NPP2 Use & Disclosure.

In 2008 the Australian Law Reform Commission recognised that disclosure of information to 'a person responsible for an individual' can occur within current privacy law. If a situation arises where a carer is seeking access to a patient's health information, practices are encouraged to contact their medical defence organisation for advice before such access is granted.

Individual records are advised for all family members but especially for children whose parents have separated where care must be taken that sensitive demographic information relating to either partner is not recorded on the demographic sheet. Significant court orders relating to custody and guardianship should be recorded as an alert on the children's records.

External Doctors and Health Care Institutions

Direct the query to the patient's doctor and or the practice manager/principal doctor.

Police/ Solicitors

Police and solicitors must obtain a case specific signed patient consent (or subpoena, court order or search warrant) for release of information. The request is directed to the doctor.

Health Insurance Companies /Workers Compensation/ Social Welfare Agencies

Depending on the specific circumstances information may be need to be provided. It is recommended that these requests are referred to the Doctor.

It is important that organisations tell individuals what could be done with their personal health information and if it is within the reasonable expectation of the patient then personal health information may be disclosed. Doctors may need to discuss such requests with the patient and perhaps their medical defence organisation.

Employers

If the patient has signed consent to release information for a pre-employment questionnaire or similar report then direct the request to the treating doctor.

Government Agencies - Medicare/Dept. Veterans Affairs

Depending on the specific circumstances information may be need to be provided. It is recommended that doctors discuss such issues with the medical defence organisations.

State Registrar of Births, Deaths and Marriages

Death certificates are usually issued by the treating doctor.

Centrelink

There are a large number of Centrelink forms (treating doctor's reports) which are usually completed in conjunction with the patient consultation

Accounts/ Debt Collection

The practice must maintain privacy of patient's financial accounts. Accounts are not stored or left visible in areas where members of the public have unrestricted access.

Accounts must not contain any clinical information. Invoices and statements should be reviewed prior to forwarding to third parties such as insurance companies or debt collection agencies.

Outstanding account queries or disputes should be directed to the practice manager/bookkeeper or principal.

Hint: Practices may like define an adequate period of time between the initial account and pursuing aggressive collection.

Third Parties such as Medical & Nursing Students

This practice does participate in medical/nursing student education.
The practice acknowledges that some patients may not wish to have their personal health information accessed for educational purposes.

The practice always advises patients of impending student involvement in practice activities and seeks to obtain patient consent prior to the consultation (not in the presence of the third party). The practice respects the patient's right to privacy.

Researchers/Quality Assurance Programs

Where the practice seeks to participate in human research activities and/or continuous quality improvement (CQI) activities, patient anonymity will be protected. The practice will also seek and retain a copy of patient consent to any specific data collection for research purposes.

Research requests are to be approved by the Practice Principal/ practice partners and must have approval from a Human Research Ethics Committee (HREC) constituted under the NH&MRC guidelines. A copy of this approval will be retained by the practice.

Practice accreditation is a recognised peer review process and the reviewing of medical records for accreditation purposes has been deemed as a "secondary purpose" by the Office of the Federal Privacy Commissioner. As a consequence patients are not required to provide consent.

Patients should be advised of the ways in which their health information may be used (including for accreditation purposes) via a sign in the waiting room and the practice information brochure.

Media

Please direct all enquiries to Practice Manger/ Principal. Staff must not release any information unless it has been authorised by the Practice Manager/ Principal and patient consent has been obtained.

International

Where patient consent is provided then information may be sent overseas however the practice is under no obligation to supply any patient information upon receipt of an international subpoena.

NPP9 Transborder Data Flows

Disease Registers

This practice submits patient data to various disease specific registers (cervical, breast bowel screening etc) to assist with preventative health management.
Consent is required from the patient with the option of opting in or opting out. Patients are advised of this via a sign in the waiting area and in the practice's information leaflet.

Telephone Calls

Requests for patient information are to be treated with care and no information is to be given out without adherence to the following procedure:

Take the telephone number, name (and address) of the person calling and forward this onto the treating doctor/principal or Practice Manager where appropriate,