Privacy and Security of Personal Health Information

Policy

This practice is bound by the Federal Privacy Act (1998) and National Privacy Principles.

'Personal health information' is a particular subset of personal information and can include any information collected to provide a health service.

This information includes medical details, family information, name, address, employment and other demographic data, past medical and social history, current health issues and future medical care, Medicare number, accounts details and any health information such as medical or personal opinion about a person's health, disability or health status.

It includes the formal medical record whether written or electronic and information held or recorded on any other medium e.g. letter, fax, or electronically or information conveyed verbally.

Our practice has a designated person, the Office Manager with primary responsibility for the practice's electronic systems, computer security and adherence to protocols as outlined in our Computer Information Security policy. Tasks may be delegated to others.

Our security policies and procedures regarding the confidentiality of patient health records and information are documented and our practice team are informed about these at induction.

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

For each patient we have an individual patient health record (paper, electronic or a combination of both, "Hybrid") containing all clinical information held by our practice relating to that patient. The Practice ensures the protection of all information contained therein. Our patient health records can be accessed by an appropriate team member when required.

Procedure

Doctors, Allied Health Practitioners and all other staff and contractors associated with this Practice have a duty to maintain the privacy of personal health information and related financial information. The privacy of this information is every patients right.

Oxford Street Medical Centre

Practice Privacy Policy

Policy

National Privacy Principle 5 requires our practice to have a document that clearly sets out its policies on handling personal information, including health information.

Our Privacy statement informs patients about how their health information will be used including sending to other organizations to which the practice usually discloses patient health information and any law that requires the particular information to be collected. A signed privacy copy of their consent is scanned onto the individual patients' notes.

Procedure

We inform our patients about our practice's policies regarding the collection and management of their personal health information via:

- A sign at reception
- Our patient information sheet
- New patient forms- "Consent for the collection and use of information"
- Verbally if necessary

The privacy policy sign outlines

- What information is collected
- Why information is collected
- How the practice maintains the security of information held at the practice
- The range of people within the practice team (e.g. GPs, general practice nurses, students and allied health professionals), who may have access to patient health records and the scope of that access
- The procedures for patients to gain access to their own health information on request.
- The way the practice gains patient consent before disclosing their personal health information to third parties
- The process of providing health information to another medical practice should patients request that
- The use of patient health information for quality assurance, and professional development
- The procedure for informing new patients about privacy arrangements
- The way the practice addresses complaints about privacy related matters
- The practice's policy for retaining patient health records.

A collection statement sets out the following information:

- The identity of the practice
- The fact that patients can access their own health information
- The purpose for which the information is collected
- Other organizations to which the practice usually discloses patient health information
- Any law that requires the particular information to be collected (e.g. notifiable disease)
- The main consequence for the individual patient, if important health information is not provided.

Patient consent for the collection and use of health information is obtained on the first visit.

Once signed this form is scanned into the patient's record.

The maintenance of privacy requires that any information regarding individual patients, including staff members who may be patients, may not be disclosed either verbally, in writing, in electronic form, by copying either at the Practice or outside it, during or outside work hours, except for strictly authorised use, within the patient care context at this Practice or as legally directed.

There are no degrees of privacy. All patient information must be considered private and confidential, even that which is seen or heard and therefore is not to be disclosed to family, staff or others without the patient's approval. This is considered health information and as such it must be protected under the Privacy Act.

Any information given to unauthorised personnel will result in disciplinary action. Each staff member is bound by his/her privacy clause contained with the employment agreement which is signed upon commencement of employment at this Practice. (Refer to Human Resource Management)

Personal health information is kept where staff supervision is easily provided and kept out of view and access by the public e.g. not left exposed on the reception desk, or left unattended in consulting or treatment rooms.

Practice computers and servers comply with the RACGP computer security checklist and we have a sound backup system and a contingency plan to protect the practice from loss of data. (Refer Section - Computer information security).

Care is taken that the general public cannot see or access computer screens that display information about other individuals. To minimize this risk automated screen

savers should be engaged. Privacy screens are filled to reception 2 computer screen to block the view of patients when making appointments.

Members of the practice team have different levels of access to patient health information. (Refer Section Computer Information Security) To protect the security of health information, GPs and other practice staff do not give their computer passwords to others in the team.

Reception and other Practice staff are aware that conversations in the main reception area can often be overheard in the waiting room and as such staff should avoid discussing confidential and sensitive patient information in this area. To help minimize this potential risk - music is played continuously in the waiting room to block out sound in the administration area.

Whenever sensitive documentation is discarded the practice uses an appropriate method of destruction – confidential cross-shredding.

Correspondence

Electronic information is transmitted over the public network in an encrypted format using secure messaging software. Where medical information is sent by post the use of secure registered postage hand delivered to Post Office for stamping, or a courier service, is determined on a case by case basis.

Copies of receipts are entered into patient electronic file.

Items for collection of postage are left in a secure area not in view of the public.

Facsimile

Facsimile, printers and other electronic communication devices in the practice are located in areas that are only accessible to authorised staff.

All faxes containing confidential information are sent to fax numbers after ensuring the recipient is the designated receiver.

Write, “Confidential” on the fact coversheet

Check the number dialed before pressing ‘SEND’

Faxes received are managed according to incoming correspondence protocols.

The practice uses a fax disclaimer notice on outgoing faxes that affiliates with the practice.

Emails

Emails are sent at risk of being intercepted. Patient information may only be sent via email if it is securely encrypted according to industry and best practice standards. At this stage this practice does not send confidential health info via email.

Patient Consultations:

Patient privacy and security of information is maximized during consultations by closing consulting room doors. All examination couches, including those in the treatment room, have privacy curtains.

When consulting, treatment room or consulting room doors are closed - prior to entering, staff should either knock and wait for a response or alternatively contact the relevant person by internal phone, if important enough to interrupt a consultation.

It is the doctor's/nurse's responsibility to ensure that prescription paper, medical records and related personal patient information is kept secure and private, if they need to leave the room during a consultation or when they leave their consulting/treatment room.

Medical Records:

The physical medical 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 Commonwealth Privacy and State Health Records Acts. Requests for access to the medical record will be acted upon only if received in written format.

Both active and inactive patient health records are kept and stored securely. (Refer Retention of records and Archiving)

Paper based Records

Security is maintained for paper based medical files at all times. During practice open hours the reception filing areas are supervised. These records are only retrieved by authorised practice staff.

Records are never to be left in public or unauthorised areas of the Practice. If a doctor has borrowed a record, it is to be kept inside the consulting room in a file cabinet or returned to be filed in the office area, on the same day.

Computerised Records

Our practice is on the path to being 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.

Computer Information Security

Policy:

Our practice has systems in place to protect the privacy, security, quality and integrity of the data held electronically. Our security policies and procedures are updated when changes occur.

The Office Manager has designated responsibility for overseeing the maintenance of our computer security and our electronic systems.

All clinical staff have access to a computer to document clinical care. For medico-legal reasons, and to provide evidence of items billed, staff, nurses and doctors always log in under their own passwords to document care activities they have undertaken.

Our practice ensures that our practice computers and servers comply with the RACGP computer security checklist and that:

- Computers are only accessible via individual password access to those in the practice team who have appropriate levels of authorization
- Computers have screen savers or other automated privacy protection devices are enabled to prevent unauthorised access to computers
- Servers are backed up and checked daily, consistent with a documented business continuity plan
- Back up information is stored in a secure off site environment
- Computers are protected by antivirus software that is installed and updated regularly
- Computers connected to the internet are protected by appropriate hardware/software firewalls
- We have a business continuity plan that has been developed, tested and documented

Electronic data transmission of patient health information from our practice is in a secure format.

Our practice has the following information to support the computer security policy:

- Current asset register documenting hardware and software including software license keys
- Maintenance, backup including test restoration, faults, virus scans
- Folder with warranties, invoices/receipts, maintenance agreements

This Practice reserves the right to check individual's Computer System history as a precaution to fraud, workplace harassment or breaches of confidence by employees. Inappropriate use of the Practice Computer Systems, breaches of Practice Computer Security will be fully investigated and may be grounds for dismissal.

This practice has a sound backup system and a contingency plan to protect practice information in the event of an adverse incident, such as a system crash or power failure. This plan encompasses all critical areas of the practice's operations such as making appointments, billing patients and collecting patient health information. This plan is tested on a regular basis to ensure backup protocols work properly so that the practice can continue to operate in the event of a computer failure of power outage.

Procedure:

The practice computer security manual and protocols is a separate folder and based on the RACGP Computer Security Guidance.

We have the following items available to enable the practice to operate in the event of a power failure - located in reception:

- Torches
- Paper prescription pads/sick certificates etc
- Appointments schedule printout and manual book
- Letterhead
- Consultation notes
- Manual credit card/payment/Medicare processing equipment
- Emergency numbers

Request for Health Information to a 3rd Party:

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 there is not signed authorization and the patient request form is not obtained the practice is not legally obliged to release health information.

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

An organization 'holds' health information if it is in their possession or control. If you have received reports or other health information from another organization 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. 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

We only transfer or release patient information to a third party once the consent to share information has been signed.

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, auctioning 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. See notice on waiting room wall.

As a rule no patient information is to be released to a 3rd party unless the patient 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.

Written requests should be noted in the patient's medical record, and also documented.

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, 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.

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 original 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 when sent to health organizations.

Subpoena, Court order, Coroner Search Warrant

Note the date of court case and date of request received in the medical record. Depending on whether a physical or an electronic copy of the record is required follow procedures as describes above.

If the original is to be transported by a secure courier service ensure a copy is mad in case of loss of the original during transport. Ensure that the court returns the record after review.

Relatives/Friends

A patient may authorize another person to be given access if they have the legal right and a signed authority. See NPP2

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 rises where a carer is seeking access to a patient's health information, this practice is encouraged to contact their medical defence organization for advice before such access is granted.

Individual records are taken for all family members. We have to take extreme care in dealing with the situation 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 & Health Care institutions

Direct the query to the patient's doctor and or the 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 need to be provided. It is recommended that these requests be referred to the Doctor.

It is important that organizations 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 organization.

Employers

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

Government Agencies

Medicare / Deparment of Veterans Affairs

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

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 doctors reports), which are usually completed in conjunction with the patient's 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 Office Manager/ Practice principal.

Students (Medical & Nursing)

The practice always advises patients of impending student involvement in practice activities and seeks to obtain patient consent accordingly. The practice respects the patients right to privacy.

Researches/Quality Assurance Programs

If and where the practice seeks to participate in human research activities and/or continuous quality improvement (CQI) activities, patient anonymity will be protected.

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

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.

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 practices information leaflet.

Telephone Calls

Requests for patient information are to be treated with great 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/nurse/principal or Office manager where appropriate.

Patients Request for Access to Personal Health Information Under the Privacy Legislation

The information forms part of the patient's medical record, hence access is permitted under privacy law.

Note: Amendments to the Privacy Act apply to information collected after 21st December 2001, however they also apply to data collected prior to this date provided it is still in use and readily accessible.

We respect an individual's privacy and allow access to information via personal viewing in a secure private area. This patient may take notes of the content of their record or may be given a photocopy of the requested information. A GP may explain the contents of their record if required. An administrative charge may be applied, at the GP's discretion and in consultation with the Privacy Officer, e.g. for photocopying a record, X-Rays and for staff time involved in processing request.

Procedure

A notice is displayed in our waiting room advising patients of their rights of access and of our commitment to privacy legislation compliance.

Release of information is an issue between the patient and the doctor. Information will only be released according to the privacy laws and at doctor's discretion. Requested records are reviewed by the medical practitioner prior to their release and only when written authorization is obtained.

Request Received

When our patients request access to their medical record and related personal information held at this practice, we document each request and endeavour to assist patients in granting access where possible and according to the privacy legislation. Exemptions to access will be noted. Each patient or legally nominated representative will have their identification checked prior to access being granted.

A patient may make a request in writing at the practice. No reason is required to be given. The request is referred to the patient's doctor.

Once completed a record of the request is scanned in the patient record.

Request by another (not patient)

An individual may authorize another person to be given access, if they have the right e.g. legal guardian, and if they have a signed authority.

Under National Privacy Principle 2 - Use and Disclosure, a 'person responsible' for the patient (includes a partner, family members, carer, guardian or close friend), if that patient is incapable of giving or communicating consent, the 'responsible person' may apply for and be given access for appropriate care and treatment or for compassionate reasons. Identity validation applies.

The privacy act defines a 'person responsible' as a parent of the individual, a child or sibling of the individual, who is at least 18 years old, a spouse or de facto spouse, a relative (at least 18 years old) and a member of the household, a guardian or a person exercising an enduring power of attorney granted by the individual that can be exercised for that person's health, a person who has an intimate relationship with the individual or a person nominated by the individual in case of emergency.

Children

Where a young person is capable of making their own decisions regarding their privacy, they should be allowed to do so according to Federal Privacy Commissioners Privacy Guidelines. The doctor could discuss the child's record with their parent. Each case is dealt with subject to the individual's circumstances as the doctor decides in consultation with their medical defence recommendations. A parent will not necessarily have the right to their child's information.

Acknowledge Request

Each request is acknowledged with a letter sent to the patient, confirming request has been received. Send the letter within 14 days or sooner as recommended by the National Privacy Commissioner. Acknowledgment will include a statement concerning charges involved in processing the request.

Fees Charged

Discuss with the individual what information they want access to, and the likely fees, before undertaking their request for access.

While there is a general charge - we need to recognise that sometimes there are mitigating circumstances. Individuals cases are to be discussed with the doctor and/or practice manager