PRACTICE OPERATIONS MANUAL

Confidentiality and Privacy Policy

powerdiary

CONFIDENTIALITY AND PRIVACY

Here's where we describe core expectations for confidentiality and privacy, including client information management and the handling of third party requests.

Review these policies at least annually for any needed updates.

CLIENT CONFIDENTIALITY

Purpose

The purpose of this policy is to ensure that all employees are trained and understand that all client information is private and confidential. Employees are responsible for maintaining client privacy in accordance with all federal and local / state regulations.

Policy

Under no circumstances will employees of [Business Name] discuss, or in any way reveal client information to unapproved employees, colleagues, other clients, family or friends, whether at the practice or outside of it, such as in the home or at social occasions. This includes client accounts, appointments, referral letters or any other clinical documentation.

[Business Name] practitioners and other employees are aware of confidentiality requirements for all client encounters and understand that significant breaches of confidentiality may provide grounds for disciplinary action or dismissal.

Procedure

Training and Orientation of Employees

All employees receive training at orientation, as well as ongoing training regarding the privacy of client information. Every employee is issued the [Business Name] privacy policy and signs a privacy statement as part of their terms and conditions of employment. (Appendix 1)

The policies and procedures of [Business Name] are explained during the onboarding of new employees, and an onboarding form is signed by each employee as confirmation that they understand and accept their obligations in relation to client privacy and the confidentiality of information.

CONFIDENTIALITY AND PRIVACY

CLIENT INFORMATION MANAGEMENT

Purpose

The purpose of this policy is to clearly state protocol for handling personal information, including health information.

Policy

[Business Name] employees have a responsibility to maintain the privacy of personal health information and related financial information. The privacy of this information is every client's right.

This policy outlines how the practice handles personal information collected (including health information) and how the security of this information is protected. A privacy statement is available to clients and anyone who requests it. (Appendix 2)

There are no degrees of privacy. All client information, including the information of employees who may be clients, must be considered private and confidential, even that which is seen or heard. Therefore, such information is not to be disclosed to family, friends, employees or others without the client's approval. Sometimes details about a client's medical history or other contextual information, such as details of an appointment, can identify them- even if no name is attached to that information. This is still considered health information and it must be protected. Client information may not be disclosed either verbally, in writing, in electronic form, or by copying either at the practice or outside it, during or outside work hours, except for strictly approved use within the client care context, or as legally directed.

Privacy Statement

This statement informs clients how their health information will be used. This includes the sharing of information to other organisations to which the practice usually discloses client health information, and any law that requires the particular information to be collected. Client consent to the handling and sharing of health information should be provided at an early stage in the process of client care. Clients should be made aware of the collection statement (Appendix 2) when giving consent to share health information.

In general, quality improvement or audit activities for the purpose of seeking to improve the delivery of a particular treatment or service is considered a directly related secondary purpose for information use or disclosure. Specific consent for this use of client health information is not required.

Procedure

Informed Consent

Clients are informed of practice policies regarding the collection and management of their personal health information via:

- Signage at reception
- Brochure/s in the waiting area
- New client forms (Appendix 1 and 2)
- Verbally, if appropriate
- Practice website

Prior to a client signing consent to the release of health information, clients are made aware that they can request a full copy of the privacy policy and collection statement.

CONFIDENTIALITY AND PRIVACY

CLIENT INFORMATION MANAGEMENT

Treatment Rooms

When treatment room or administration office doors are closed prior to entering, employees should either knock and wait for a response, or alternatively contact the relevant person by using an internal phone or messaging system.

It is the practitioner / health care professional's responsibility to ensure that records and related client information is kept secure at all times, including whenever they are not in attendance in a consulting / treatment room.

Client privacy and security of information is enhanced during consultations by closing treatment room doors. All examination benches have curtains or privacy screens.

Staff Access

[Business Name] client health records can be accessed by an appropriate team member when required. All client health records are electronic and accessible through Power Diary by appropriate employees.

[Business Name] employees have different levels of digital access to client health information. To protect the security of health information, employees do not give their computer / Power Diary passwords to others in the team.

Personal health information should be kept where employee supervision is easily provided, and kept out of public view and access.

Computer Security

Active and inactive client health records are kept and stored securely within Power Diary.

This 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 employees are trained in computer security policies and procedures.

[Business Name] computers and servers comply with computer security standards. A sound back up system and a contingency plan is in place to protect the practice from loss of data.

Care should be taken that the general public cannot see or access computer screens that display information about other individuals. To reduce this risk, automated screen savers should be engaged.

Administration Security

Reception and other practice employees should be aware that conversations in the main reception area can often be overheard in the waiting room. As such, employees should avoid discussing confidential and sensitive client information in this area.

Whenever sensitive documentation is discarded, the practice uses an appropriate method of destruction. Documents are placed in the confidential waste bin, and confidential waste is disposed of securely. All computers, memory sticks or CDs are disposed of properly by a designated employee.

[Business Name] employees ensure that all forms of client information are not visible to the public.

CONFIDENTIALITY AND PRIVACY

CLIENT INFORMATION MANAGEMENT

Correspondence

Electronic information is transmitted over the public network in an encrypted format using secure messaging software. Where client information is sent by mail, the use of secure postage or a courier service is determined on a case by case basis. Return address states the physical or post office address, but the practice name is not identified on the envelope.

Incoming client correspondence and diagnostic results are opened by a designated employee.
Items for collection or postage are left in a secure area out of public view.

Facsimile, printers and other electronic communication devices in the practice are located in areas that are only accessible to practitioners and other approved staff. Faxing is point to point, and will therefore usually only be transmitted to one location.

All faxes containing confidential information are sent to fax numbers after ensuring the recipient is the designated receiver. Each fax is accompanied by a cover sheet, the cover sheet includes the words “confidential” and a fax disclaimer notice that affiliates with [Business Name].

Emails are sent via various nodes and are at risk of being intercepted. Client information may only be sent via email if it is securely encrypted according to industry and best practice standards.

CONFIDENTIALITY AND PRIVACY

THIRD PARTY REQUESTS

Purpose

The purpose of this policy is to define the procedures for timely, approved and secure transfer of client health information in relation to valid requests.

Policy

Ensure that final policies are compliant with regulations in your country.

Requests for third party access to client records should be initiated by either receipt of correspondence from a lawyer, government agency, another source including the examples listed below, or by the client with a written request. Where a client's written request and / or signed approval is not obtained, the practice is not legally required to release information without a court order.

Requests for access may be received from various third parties including:

- Subpoena / court order / coroner / search warrant
- Relatives / friends / caregivers
- External practitioners & healthcare institutions
- Police / lawyers
- Health insurance companies / workers compensation / social welfare agencies
- Employers
- Government agencies
- Accounts / debt collection
- Research / quality assurance programs
- Media

Procedure

Subpoena, Court Order, Coroner or Search Warrant

Note the date of the court case and date the request is received in the client's record. Depending on whether a physical or electronic copy of the record is required, follow procedures as described in the section "Releasing Records" of this policy.

On occasion, an employee may be required to accompany the record to court, or a secure courier service may be adequate. If the original record 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 client may approve another person to be given access if they have the legal right and a signed authority. Disclosure of information to 'a person responsible for an individual' may be permitted in accordance with the law. If a situation arises where a carer is seeking access to a client's health information, practices are encouraged to contact their insurer for advice before such access is granted.

Individual records are advised for all family members, but especially for children whose parents have separated. 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 Health Practitioners

Direct the request to the client's treating practitioner.

CONFIDENTIALITY AND PRIVACY

THIRD PARTY REQUESTS

Police or Lawyers

Police and lawyers must obtain a case-specific signed client consent (or subpoena, court order or search warrant) for release of information. The request is to be directed to the treating practitioner.

Health Insurance Companies, Workers Compensation or Social Welfare Agencies

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

It is important that the practice inform individuals regarding how their personal health information may be used, and if it is within the reasonable expectation of the client that personal health information may be disclosed. Practitioners may need to discuss such requests with the client and perhaps the practice's indemnity insurer.

Employer

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

Government Agencies

Depending on the specific circumstances, information may need to be provided to government agencies, including government-run healthcare agencies. It is recommended that treating practitioners discuss such issues with their insurer.

Government Requested Information

There are a large number of forms that a government entity may request, such as treating practitioner reports. These are usually completed in conjunction with the client in a consultation.

Accounts and Debt Collection

[Business Name] must maintain privacy of clients' 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 requests or disputes should be directed to the practitioner.

Research or Quality Assurance

Where practitioners participate in human research activities and / or continuous quality improvement (CQI) activities, client anonymity will be protected. [Business Name] will also seek and retain a copy of client consent to any specific data collection for research purposes.

Research requests are to be approved by the treating practitioner. A copy of this approval will be retained by the practice.

Media

Direct all media requests to treating practitioners. Employees must not release any information unless it has been approved by the treating practitioner and client consent has been obtained.

CONFIDENTIALITY AND PRIVACY

THIRD PARTY REQUESTS

International

Where client consent is provided, information may be sent internationally. If an international subpoena is received, check with the practice's insurer to ensure an appropriate response.

Telephone Calls

Requests for client information are to be treated with care. No information is to be given out without adherence to the following procedure:

Record the telephone number, name (and address) of the person calling and forward this to the treating practitioner, along with the reason for the request.

Releasing Records

- Ensure correct identification of the client using identifiers, name, date of birth, address or gender
- Client consent for the transfer of health information to other providers or agencies is obtained on the first visit and retained on file
- Requests for release of client information should be made in writing, and signed authority from the client should be included
- Written requests are noted in the client's record
- Requested records are to be reviewed by the treating practitioner prior to their release to a third party
- [Business Name] may specify a charge to be incurred by the client or third party, to meet the cost of time spent preparing the report or photocopying / printing the record
- [Business Name] retains a record of all requests for access to client information, including transfers to other health practitioners
- Where hard copy records are sent to clients or third parties, only copies are forwarded- if originals are required, copies are made in case of loss
- Security of any health information requested is maintained when transferring requested records
- Electronic data transmission of client health information from the practice is in a secure format

CONFIDENTIALITY AND PRIVACY

TRANSFER OF CLIENT RECORDS

Purpose

The purpose of this policy is to guide employees in the process of timely, approved and secure transfer of records.

Policy

Ensure that final policies are compliant with regulations in your country.

Transfer of records from this practice can occur in the following instances:

- For legal reasons, as when record is subpoenaed to court
- When a client asks for their record to be transferred to another practice, due to moving residence or for other reasons
- Where an individual record report is requested from another source
- Where the practitioner is retiring and the practice is closing

Procedure

Request for Legal Reasons

Refer to third party access

Request to Transfer to Another Facility / Practitioner

In accordance with privacy regulations, a request to transfer records must be signed by the client who is giving authority to transfer their records.

The request form should contain:

- The name of the receiving practitioner or facility
- The name, address (both current and former if applicable) and date of birth of the client whose record is required
- The reason for the request

When fulfilling a request, this practice may choose to either

- Prepare a summary letter (manually or via clinical software) and include copies of relevant correspondence and results pertinent to the ongoing management of the client
- Make a copy of the record and dispatch the copy to the new practice, retaining the original on site for a minimum of 7 years

The requesting clinic is advised if a summary or a copy of the full client record will be transferred. If the requesting clinic has a preference, the format can be negotiated.

If there are any expenses related to the transfer, the requesting practice is advised prior to sending the records. Once the fee has been paid, requests are processed as soon as possible.

The client's signed request letter / form and a notation that the client has transferred is made on the record. Include the name and address of the new practice and the dispatch details (such as via priority mail, confidential courier or in an electronic form).

Electronic data transmission of client health information from the practice is in a secure format.

All reasonable steps are taken to protect the health information from loss and unapproved disclosure during the transfer.

CONFIDENTIALITY AND PRIVACY

CLIENT ACCESS TO THEIR HEALTH INFORMATION

Purpose

The purpose of this policy is for [Business Name] employees to understand and comply with client rights in regard to accessing a client's own health information

Definitions

Person Responsible: 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.

Policy

Ensure that final policies are compliant with regulations in your country.

Clients have the right to access their personal health information. This principle obliges health practices and other parties that hold health information about a person to grant access to their information on request, subject to certain exceptions and payment of fees (if any).

[Business Name] has a privacy policy in place that outlines the management of health information, and the steps a client must take to access their health information. This includes the different forms of access and the applicable time frames and fees.

[Business Name] respects each client's privacy, and allows access to information via personal viewing in a secure private area. The client may take notes of the content of their record, or may be given a photocopy of the requested information. A practitioner may explain the contents of the record to the client if required. An administrative charge may be applied, at the practitioner's discretion.

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

Procedure

When [Business Name] clients request access to their record and related personal information, the procedure is as follows:

- Document each request in the client's health record
- Assist clients in granting access where possible and according to privacy laws
- Exemptions to access will be noted
- Each client or legally nominated representative will have their identification checked prior to access being granted

Request by a Client

A client may make a request verbally at the practice, via telephone or in writing. No reason is required. The request is referred to the client's practitioner or delegated employee.

A Request for Personal Health Information form is completed to ensure correct processing.

Once completed, a record of the request is filed / scanned in the client record.

CONFIDENTIALITY AND PRIVACY

CLIENT ACCESS TO THEIR HEALTH INFORMATION

Request by Another (Not the Client)

A client may approve another person to be given access, if they have the right and if they have a signed authority.

A person responsible for the client, if that client is incapable of giving or communicating consent, may apply for and be given access to information. Such access will be approved by the treating practitioner. Identity validation applies.

Children

Where a young person is capable of making their own decisions regarding their privacy, they should be allowed to do so, each case is dealt with subject to the individual's circumstances. A parent will not necessarily have the right to their child's information.

Deceased Person

A request for access may be allowed for a deceased client's legal representative if privacy law requirements have been met.

Acknowledge Request

A letter must be sent to the client acknowledging a request for information within 14 days of receipt of the request.

Fees

Fees that [Business Name] charge for providing access to client information are not excessive and do not apply to the mere submission of a request for access.

If [Business Name] incurs substantial costs in meeting a request for access, then a reasonable fee will be charged.

Collate and Assess Information

Paper records will be retrieved and/or the practitioner will access the computer record. Refer to the client request to help identify what information is to be given to the client.

Data may be withheld for the following reasons:

- Where access would pose a serious threat to the life or health of any individual
- Where the privacy of others may be affected
- If a request is frivolous or vexatious
- If information relates to existing or anticipated legal proceedings
- If access would prejudice negotiations with the individual
- If access would be unlawful
- Where denying access is required or granted by law

Access Denied

Reasons for denied access must be given to the client in writing. In some cases, refusal of access may be in part or full.

If a request for access is denied, an intermediary, such as a medical indemnity company, may operate as a facilitator to provide sufficient access to meet the needs of both the client and the practitioner.

CONFIDENTIALITY AND PRIVACY

CLIENT ACCESS TO THEIR HEALTH INFORMATION

Providing Access

Personal health information may be accessed in the following ways:

- Viewing and inspecting information
- Viewing inspecting and talking through contents with the practitioner
- Taking notes
- Obtaining a copy (photocopy or an electronic printout from a computer)
- Listening to audio or viewing video
- Information may be faxed, emailed or mailed to the client

Check Identity

- Ensure a visible form of ID is presented by the person seeking access- note the details
- Does the person have the authority to gain access?
- Check age, legal guardian documents- is the person an approved representative?

If the client is viewing their own data, supervise each viewing so that the client is not disturbed and no data goes missing.

If a copy is to be given to the client, ensure all pages are checked and that this is noted in the client's file.

If a practitioner is to explain the contents to a client, ensure an appointment time is made.

Request to Correct Information

A client may ask to have their personal health information amended if they consider that it is not up to date, accurate and complete.

[Business Name] always attempts to correct this information. Corrections are attached to the original health record.

Where there is a disagreement about whether the information is indeed correct, [Business Name] attaches a statement to the original record outlining the client's claims.

Time Frames

Acknowledge requests within 14 days, complete the request within 30 days.

CONFIDENTIALITY AND PRIVACY

DATA BREACH NOTIFICATION

Purpose

The purpose of this policy is to advise [Business Name] employees on actions required if a data breach occurs.

Definitions

Data Breach: Personal information that an entity holds that is subject to unapproved access. This can be malicious action, human error or a failure in handling or security.

Personal Information: Information about an identified individual or an individual who is identifiable from the information.

Policy

A data breach occurs when personal information that [Business Name] holds is subject to unapproved access or disclosure, or is lost. Data breaches can happen to any practice.

[Business Name] can reduce the reputational impact of a data breach by effectively reducing the risk of harm to affected individuals, and by demonstrating accountability in their data breach response.

Procedure

[Business Names] employees understand the importance of being transparent when a data breach, which is likely to cause serious harm to affected individuals, occurs. Transparency enables individuals to take steps to reduce their risk of harm. It also demonstrates that [Business Name] takes their responsibility to protect personal information seriously, which is integral to building and maintaining trust in [Business Name]'s personal information handling capability.

Examples of Data Breach

- Loss or theft of a physical device (such as a laptop or paper records)
- Unapproved access by an employee or other person
- Inadvertent disclosure due to human error, such as a fax being sent to an incorrect number
- Disclosure to a third party due to inadequate verification process

Consequences of Breach

- Financial loss
- Potential damage to clients' reputations
- Damage to clients' physical or mental well being

Response to Data Breach

As data breaches can be caused or exacerbated by many factors, there is no single way of responding to a data breach. Each breach will need to be dealt with on a case-by-case basis, with an understanding of the risks posed by a breach and the actions that would be most effective in reducing or removing these risks.

Generally, the actions taken following a data breach should follow four key steps:

- Contain the data breach to prevent any further compromise of personal information
- Assess the data breach by gathering the facts and evaluating the risks, including potential harm to affected individuals and, where possible, taking action to remediate any risk of harm
- Notify individuals, government bodies and medical indemnity if required
- Review the incident and consider what actions can be taken to prevent future breaches

CONFIDENTIALITY AND PRIVACY

DATA BREACH NOTIFICATION

[Business Name] takes each data breach or suspected data breach seriously, and moves immediately to contain, assess and remediate the incident. Breaches that may initially seem immaterial may be significant when their full implications are assessed.

Steps will be taken to contain, assess, and notify either simultaneously or in quick succession. In some cases, it may be appropriate to notify individuals immediately, before containment or assessment of the breach occurs.

[Business Name] determines how to respond on a case-by-case basis. Depending on the breach, not all steps may be necessary, or some steps may be combined. In some cases, additional steps may be taken that are specific to the nature of the breach.

Reporting Data Breaches

What to include in a data breach report:

- Your practice or agency's name and contact details
- Description of the data breach
- Kinds of information involved
- Recommendations about the steps individuals should take in response to the data breach

CONFIDENTIALITY AND PRIVACY

APPENDIX 1

Privacy and Confidentiality Statement

I _____ understand [Business Name]'s requirement to protect the privacy of information as detailed below:

All client 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 treating practitioner or designated privacy officer, and according to privacy law.

This privacy statement is binding even if I am no longer employed by [Business Name].

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

Full Legal Name (in block letters) _____

Signature _____Date:_____

Witnessed by, Full Legal Name (in block letters) _____

Signature _____Date:_____

CONFIDENTIALITY AND PRIVACY

APPENDIX 2

Privacy and Collection Statement for Clients

This privacy statement is to provide information to [Business Name] clients as to how your personal information (including health information) is collected and used within [Business Name], and the circumstances in which we may share it with third parties.

When you register as a client of [Business Name], you provide consent for our practitioners and staff to access and use your personal information so they can provide you with the best possible healthcare. Only employees 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.

[Business Name] 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 business processes (such as staff training).

Information Collected

The information we will collect about you includes:

- Names, date of birth, addresses, contact details
- Medical information relevant to your treatment, including medical history, medications, allergies, adverse events, vaccinations, social history, family history and risk factors
- Medicare number (where available) for identification and claiming purposes
- Healthcare identifiers
- Health fund details, if applicable
- Credit card details

[Business Name] will collect your personal information:

1. When you make your first appointment, our staff will collect your personal and demographic information via your registration.
2. During the course of providing healthcare services, we may collect further personal information.
3. With your consent and if services are available, Information may also be collected through the following eHealth services ***Specify which, if any, eHealth services your practice participates in, such as a prescription service.
4. We may also collect your personal information when you send us an email or SMS, telephone us, make an online appointment or communicate with us using social media.
5. 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 insurer (as necessary). ***Specify relevant insurer or government agency information according to your country

Information We May Share

We sometimes share your personal information:

- With third parties who work with [Business Name] for business purposes, such as accreditation agencies or information technology providers – these third parties are required to comply with Federal and State Legislation as well as this policy
- With other healthcare providers
- When it is required or approved by law (such as court subpoenas)
- When it is necessary to lessen or prevent a serious threat to a client's life, health or safety or public health or safety, or it is impractical to obtain the client's consent
- To assist in locating a missing person

CONFIDENTIALITY AND PRIVACY

APPENDIX 2

- 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 (such as some diseases which may require mandatory notification)

Only people that need to access your information will be able to do so. Other than in the course of providing healthcare services or as otherwise described in this policy, [Business Name] will not share personal information with any third party without your consent.

[Business Name] 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 [Business Name] directly.

Our practice stores all personal information securely.

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

Your Right to Access

[Business Name] acknowledges clients may request access to their health records. We require you to put this request in writing in person, mail or email. All requests must be accompanied by photo ID. Our practice will respond within 10 working days. There is an administration cost of $XX.XX for a full copy of medical records and $XX.XX for a series of test results or health summary.

[Business Name] will take 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