Privacy and confidentiality

The Privacy Amendment (Private Sector) Act 2000 extends the operation of the Privacy Act 1988 to cover the private health sector throughout Australia.

The Privacy Act requires our practice to abide by the 10 National Privacy Principles (NPPs):

NPP 1	Collection
NPP 2	Use and Disclosure
NPP 3	Data Quality
NPP 4	Data Security
NPP 5	Openness
NPP 6	Access and Correction
NPP 7	Identifiers
NPP 8	Anonymity
NPP 9	Transborder Data Flows
NPP 10	Sensitive Information

For further information regarding complying with the legislation visit the website of the Office of the National Privacy Commissioner

Patient health information

The maintenance of privacy requires that any information regarding individual patients, including staff members who may be patients, must not be disclosed in any form (verbally, in writing, electronic forms inside/outside our practice) except for strictly authorised use within the patient care context at our practice or as legally directed.

Health records must be kept where constant staff supervision is easily provided. Personal health information must be kept out of view and must not be accessible by the public.

All patient health information must be considered private and confidential, and therefore must not be disclosed to family, friends, staff or others without the patient's consent. This information includes medical details, family information, address, employment and other demographic and accounts data obtained via reception. Any information given to unauthorised personnel will result in disciplinary action, possible dismissal and other legal consequences.

Each staff member must sign a confidentiality agreement on commencement of employment and further information is provided in Human resource management.

In addition to Federal legislation, our practice also complies with State or Territory legislation.

Care should be taken that individuals cannot see computer screens showing information about other individuals. Screensavers or other methods of protecting information must be engaged.

Access to computerised patient information must be strictly controlled with personal logins/passwords. Staff must not disclose passwords to unauthorised persons. Screens need to be left cleared when information is not being used. Terminals must also be logged off when the computer is left unattended for a significant period of time.

Items for the pathology couriers or other pick-ups must not be left in public view.

Practice procedure

In our practice, to ensure the maintenance of privacy, active paper health records are stored in numerically coded charts in the Practice Manager's office, and archived paper health records are stored in the store room at the rear of the practice or in the Practice Manager's Office.

In our practice, computer screens are positioned so that individuals cannot see information about other individuals, access to computerised patient information is strictly controlled with passwords and personal logins, automatic screen savers and computer terminals are logged off when the computer is left unattended for a significant period of time.

In our practice, items for pathology couriers or other pickups are left in the Treatment in specially marked containers room.