Management of Patient Health Information Policy

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 are kept where constant staff supervision is easily provided. Personal health information is kept out of view and is not be accessible by the public. (Criterion 4.2.2)

All patient health information is considered private and confidential, and therefore is not to 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 this, levels of information accessible to staff is in line with their position and job role.

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

Care is taken to ensure that individuals cannot see computer screens showing information about other individuals. Screensavers or other methods of protecting information is engaged and requires login passwords on return.

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

Items for the pathology couriers or other pickups are not be left in public view and dealt with promptly.

All information stored electronically is protected by a firewall and is backed up daily. All firewalls and passwords are set to a very high standard and managed by an independent IT provider who specialises in Medical practices.

As follows is a link to the National privacy principles which we are governed by and actively follow:

https://www.oaic.gov.au/resources/privacy-law/privacy-archive/privacy-resources-archive/privacy-fact-sheet-2-national-privacy-principles.pdf