Privacy Policy MAG023

Subject: :	Privacy Policy
Scope of Procedure:	The purpose of this policy is to ensure best practice in the management of information we collect, hold, use or disclose.
Responsible for Review:	Executive
Approved by:	Board Macquarie Anaesthetic Group
Distribution:	Practice Wide
Location:	Macquarie Anaesthetic Group – General Documents Policy a Procedure.

Reference: Australian Medical Board (NSW) "*Privacy Kit*", June 2016.
The Health Records and Information Privacy Act 2002 (NSW).
The Privacy Act 1988.
Presidian Legal Publications "*Data Breach Notification Scheme: Guide & Toolkit". (*Privacy Act 1988 (Cth), Part IIIC)

Terminology adopted in the Privacy Laws

Health Service
Health service means an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by an individual, or the person performing it to:

- Assess, record, maintain or improve the individual's health;
- Diagnose the individual's illness or disability; or
- Dispense on prescription a drug or medical preparation by a pharmacist.

Health service providers can range from hospital and general practitioners to organisations that may not traditionally have been considered health services providers such as gyms and weight loss clinics.

Collection
An organisation collects personal information if it gathers, acquires or obtains information from source, by any means, in circumstances where the individual is identified or is identifiable. It includes information that:

- An organisation comes across by accident or has not asked for but nevertheless keeps;
- The organisation receives directly from the individual;
  and
- Information about an individual an organisation receives from somebody else.

Holding
An organisation holds personal information if;

- An organisation is in procession or control of the information, or
- The information is in the procession or control of a person employed or engaged by the organisation in the course of such employment or engagement.

Use
Use of personal information relates to the handling of personal within the organisation. Examples of uses of information are:

- Adding information to a data base;
- Forming an opinion based on information collected and noting it on file.

Disclosure
An organisation discloses information when it releases information outside the organisation. Examples of disclosure include:

- When an organisation gives another organisation information under contract to carry out "outsourced" function;
- When an organisation sells information to another organisation.

Personal Information
Personal information means information or an opinion (including information or an opinion forming part of a data base) whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Personal information must relate to a natural person.
A natural person is a human being rather than, for example, a company, which may in some circumstances, be recognised as a legal "person" under the law.
Personal information can range from the very sensitive (for example, political beliefs, medical history, sexual preference or medical records) to the everyday (for example, hair colour, address, phone number). The information need not be accurate, it may include opinion and speculation and it may simply be incorrect information. It doesn't matter whether the information is held in a computer database, or in paper records, or in any other medium, provided the information itself makes it clear which individual is identifiable. Whether an individual's identity is reasonably ascertainable will depend on the context and on who holds the information.

Health Information
Health information means personal information or an opinion about the:

- Health or disability (at the time) of an individual;
- Individual's expressed wishes about the future provision of health services;
- Health services provided or to be provided to an individual that is also personal information or other personal information collected to provide, or in providing a health service;
- Personal information about an individual collected in connection with the donation, or intended donation by an individual or his or her body parts, organs or body substances;
- Personal information that is genetic information arising from a health service provided to the individual in a form that is or could be predictive of the health of the individual or ant sibling, relative or descendant of the individual.

Health information can include details such as an individual's name, address, billing information and Medicare number.

Health Records and Information Privacy Act 2002 (NSW) regulates the way in which NSW public and private sector organisations collect, hold and disclose an individual's health information.

The Privacy Act 1988 sets the standard way in which organisations in the private sector collect, hold, use and disclose personal information.

All health service providers in NSW must comply with both state and federal privacy legislation.

Macquarie Anaesthetic Group is committed to best practice in relation to the management of information we collect. This practice has developed a policy to protect patient privacy in compliance with the Privacy Act 1988.

The type of information we may collect and hold includes:

- Name, address, date of birth, email and contact details of patient;
- Medicare number, health fund or DVA number;
- health fund/ insurance remittance advice
- bank/ credit card details

Other health information including:

- surgical procedure
- treating hospital
- specialist reports and test results
- relevant health history as supplied by patients
- relevant correspondence from patient or treating doctors

We generally collect personal information:

- directly from the patient. This may be via a face to face discussion, telephone conversation, email or online form;
- relative or carer;
- from third parties where the Privacy Act or other law allows- this may include but is not limited to: other members of treating team, diagnostic centres, specialists, hospitals, Medicare or health insurer.

In general, we collect, hold, use and disclose personal information for the following purposes:

- to provide a health service to the patient;
- to communicate to patient in relation to the health service being provided to them;
- to comply with our legal obligations;
- to manage our accounts and administration services, including billing, arrangements with health funds, pursuing unpaid accounts;
- for consultation with other doctors and allied health professional involved in the healthcare of the patient;
- for identification and insurance claiming;
- to liaise with health fund, government and regulatory bodies such as Medicare, the Department of Veteran's Affairs and the office of the Australian Information Commissioner (OAIC) should a privacy complaint be made against the practice.

Patients have the right to seek access to and correct personal information we hold about them.

Staff are trained and required to respect and protect patient privacy.
Responsible steps are taken to protect information held from misuse and loss and from unauthorised access, modification or disclosure.
This includes:

- password protected software system;
- secure cloud storage;
- signed confidentiality agreements by all staff;
- secure confidential waste destruction.
-

Overseas Disclosure
We may disclose personal information to the following overseas recipients:
overseas insurance providers.

Any patient questions in regards to a privacy related issues should be responded to within 30 days.
Should they be dissatisfied with our response patients have the right to refer the matter to the:
OAIC:
Phone: 1300 363 992
Email: enquires@oaic.gov.au
Fax: +61 2 9284 9666
Post: GPO Box 5218 Sydney NSW 2001
Website: www.oaic.gov.au/individuals/how-do-i-make-a -privacy-complaint

A summary of the NSW Health Records and Information Privacy Act 2002 15 Health Privacy Principles (HPPs)

Collection

1. Lawful – only collect health information for a lawful purpose. Only collect health information if it is directly related to the organisation's activities and necessary for that purpose.

2. Relevant – ensure that the health information is relevant, not excessive, accurate and up to date. Ensure that the collection does not unreasonably intrude into the personal affairs of the individual.

3. Direct – only collect health information directly from the person concerned, unless it is unreasonable or impracticable to do so.

4. Open – inform the person as to why you are collecting health information about them, what you will do with the health information, and who else might see it. Tell the person how they can see and correct their health information, and any consequences, if they decide not to provide their information to you.

If you collect health information about a person from someone else, you must still take reasonable steps to ensure that the person has been notified as described above.

Storage

5. Secure – ensure that health information is stored securely, not kept any longer than necessary, and disposed of appropriately. Information should be protected from unauthorised access, use or disclosure.

Access and Accuracy

6. Transparent – explain to the person what health information about them is being stored, why it is being used and any rights they have to access it.

7. Accessible – allow people to access their health information without unreasonable delay or expense.

8. Correct – allow people to update, correct or amend their health information where necessary.

9. Accurate – ensure that the health information is relevant and accurate before using it.

Use

10. Limited – only use health information for the purpose for which it was collected, or a directly related purpose that the person would expect. Otherwise, you generally need their consent.

Disclosure

11. Limited – only disclose health information for the purpose for which it was collected, or a directly related purpose that the person would expect. Otherwise, you generally need the individual's consent.

Identifiers and Anonymity

12. Not identified – only identify people by using unique identifiers if it is reasonably necessary to carry out your functions efficiently.

13. **Anonymous**– give people the option of receiving services from you anonymously, where this is lawful and practicable.

Transferrals and Linkage

14. **Controlled** – only transfer health information outside New South Wales in accordance with the specific requirements.

15. **Authorised** – people must expressly consent to participate in any system that links health records across more than one organisation. Only include health information about them, or disclose their identifier for the purpose of the health records linkage system, if they have expressly consented to this.

Data Breach Notification

The Data Breach (DBN) Scheme came into effect 22 February 2018.

Data Breach is when personal information held is lost or subject to unauthorised access, modification, disclosure, or other misuse or interference.

Data breaches are not limited to malicious actions, such as theft or hacking, but may arise from internal errors or failure to follow information handling policies that may cause accidental loss or disclosure.

If there is a real risk of serious harm as a result of a data breach within the practice the affected individual and the Office of the Australian Information Commissioner (OAIC) should be notified.

Any data breach should be evaluated on a case-by-case basis and decisions on actions should be taken according to the assessment of risks.

The scale and intent behind the breach is not relevant to weather a breach occurs. A breach may occur regardless of whether:

- the affected records relate to a single individual or a large number of individuals; and
- regardless of whether it is a result of an accidental employee error of a malicious third party.

Following the discovery or suspicion of a data breach the following steps should be taken;

Contain the Breach

Take whatever steps possible to immediately contain the breach.

Access whether steps can be taken to mitigate the harm to an individual may suffer a result of the breach.

Preliminary Assessment

The CEO or her delegate will conduct the initial investigation. The following information is to be collected and considered within 30 days:

- What personal information does the breach involve?
- What was the cause of the breach?
- What is the extent of the breach?
- What are the harms (to the affected individual(s) that could potentially be caused by the breach?
- How can the breach be contained?

Notification

A determination of who needs to be made aware of the breach (internally or externally) needs to be made in the preliminary stage.

It may be appropriate to notify the affected individuals immediately where there is a high level of risk to them.

If the beach appears to involve theft or other criminal activities, the police are to be notified.
Care should be taken not to destroy evidence that may be valuable in determining the cause or would allow appropriate corrective action.

Data Breach Statement
If a data breach occurs, a "Data Breach Statement" must be prepared as soon as practicably possible.
It should contain the following:

- Contact details of Practice
- Description of Breach
- Information concerned
- Recommendations of steps needed to respond to breach

An Incident Form is to be completed and forwarded to the Executive Committee.

Notification to Commissioner
If the data breach is likely to involve real risk of serious harm to individuals, or receive a high level of media attention, the Executive Committee should be notified with the intention of notifying the OAIC.

A copy of the data Breach Statement must be provided to the Commissioner and should include the following:

- Description of Breach
- Information involved in the breach
  - financial details (if applicable)
  - identity information
  - contact details
  - health information
  - other sensitive information
- recommended steps
- other entities affected

If prompt remedial action that avoids a risk of serious harm being caused, it ***will not*** be necessary to notify the Commissioner or individuals about the breach.

Information and Privacy Commission New South Wales
Phone: 02 80191600
Fax: 02 81143755
GPO Box 7011
Sydney NSW 2001
Email: privacyinfo@privacy.nsw.gov.au
Website: www.ipc.nsw.gov.au

Flowchart – Data Breach Notification Scheme
(Privacy Act 1988, Part IIIC)