The Royal College of Pathologists of Australasia
ABN 52 000 173 231

Durham Hall 207 Albion Street Surry Hills NSW 2010 Australia
Telephone 61 2 8356 5858 Facsimile 61 2 8356 5828

RCPA
The Royal College of Pathologists of Australasia

Guideline

Subject:	**Managing Privacy Information in Laboratories**
Approval Date:	March 2014, May 2018
Review Date:	May 2022
Review Committee:	Board of Directors
Number:	2/2014

In general, the Privacy Act, as well as this Guideline applies to pathologists working in the private sector. If working in the public sector, the Privacy Act will also apply when pathologists are working for a Commonwealth government agency. Separate State/Territory and International jurisdictional laws apply when working in those sectors.

This Guideline has been developed to provide guidance to pathologists on the management of personal information and privacy in their laboratories. This Guidelines focusses on obligations under the *Privacy Act 1988* (Cth) (**Privacy Act**) and in particular, under the Australian Privacy Principles (**APPs**) which form part of the Privacy Act. The APPs are divided into five parts, according to the different stages of personal information management running from the collection of personal information through to its disposal. See Appendix 1 for a full text of the thirteen APPs.

The Privacy Act also contains provisions requiring the mandatory notification of certain data breaches that affect personal information. The Privacy Commissioner refers to the mandatory obligations as Notifiable Data Breaches (NDB) scheme.

The Federal Privacy Commissioner's *Guidelines on Privacy in the Private Health Sector* discuss the application of the privacy principles in the health care setting in detail. This publication can be found on the website of the Office of the Australian Information Commissioner located at www.oaic.gov.au. The *Guidelines on Privacy in the Private Health Sector* are not legally binding. Accordingly, Fellows or Trainees should not rely on this document and should seek specific legal advice regarding compliance with the APPs. This document is intended as an educational tool only, to assist Fellows and Trainees in understanding their obligations under the APPs.

This College Guideline *Privacy Guidelines – Managing Healthcare Information In Laboratories* generally focuses on privacy principles related to pathologists and their laboratories. It also addresses the application of these principles when a pathology practice faces a change in business circumstance or closure.

This Guideline does not address the way the College as an organisation collects, uses, stores and disclosures personal information. For College privacy policy as an organisation, see Policies: *College Privacy Policy No. 1/2014.*

Australian Privacy Principles - Who is affected in the Private Sector?

In general, organisations with an annual turnover of greater than AU$3 million will need to comply with the thirteen APPs. The APPs will apply to many private sector organisations and to Commonwealth government agencies, together defined in the Privacy Act as 'APP entities'.

A business with an annual turnover of AU$3 million or less will have to comply with the Privacy Act only if it meets one of the following criteria:

- **a health service provider**; or
- trading in personal information (e.g. buying or selling a mailing list); or
- related to a business that is not a small business; or
- a contractor that provides services under a Commonwealth contract; or
- a reporting entity for the purposes of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act); or
- an operator of a residential tenancy database.

Health service providers that operate in both the public and private sectors.

Some pathologists work in both public and private hospitals/laboratories, and organisations contracted by government for some of their work, but which otherwise operate privately.

Complexities arise when services are delivered through a mix of private and public sector providers across both private and public sector sites. For example, where public and private hospitals are co-located.

Where a private health service provider works within a public hospital, it is generally the case that the medical record remains subject to management by the public sector hospital, regardless of whether clinical entries are made in those records by public or private sector providers. If the hospital is managed at a Federal level, the Privacy Act will apply. Otherwise, the relevant legislation will be the privacy laws of the State or Territory where the hospital is located.

However, if a private health service provider treats or provides laboratory services to an individual in a public hospital, but retains records (including copies) in a private laboratory or clinic or other place away from the public hospital, these records are subject to the Privacy Act.

What Information is Covered?

The Australian Privacy Principles apply to any information that is classed as “personal information”, “sensitive information” or “health information”. “Sensitive information” and “health information” which are part of “personal information” are subject to greater protection.

Personal information

“Personal information” is information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. This definition is very broad. It will cover information such as credit card details, information gathered on websites and mobile telephone numbers linked to user names and mailing lists. Data that is de-personalised or aggregated, or in some way masks the identity of the individual, is unlikely to be “personal information”.

Sensitive information

“Sensitive information” includes information about a person’s racial or ethnic origin, political or religious beliefs, philosophical beliefs, membership of professional or trade associations or unions, sexual practices and criminal record. It also includes health information.

Health Information

"Health information" is defined as follows:

- information or an opinion about the health or a disability (at any time) of an individual, about an individual's expressed wishes regarding the future provision of health services to them, or about a health service provided, or to be provided, to an individual;
- other personal information collected to provide, or in providing, a health service; or
- other personal information about an individual collected in connection with the donation, or intended donation, by the individual of their body parts, organs or body substances (including genetic information such as DNA samples).

Other Acts

The requirements under the *Victorian Health Records Act 2001,* the ACT *Health Records (Privacy and Access) Act 1997 and* the NSW *Health Records and Information Privacy Act 2002* will also apply. Consequently, the ACT, Victorian and NSW obligations for health service providers to either retain and provide storage for health records upon closure of their practice or transfer the records to another health service provider will remain.

Part 1 — Consideration of Personal Information Privacy

APP1 – Open and Transparent Management of Personal Information

Under this principle, health service providers need to have ongoing practices and policies in place to ensure that they manage personal information in an open and transparent way. Health service providers must have an APP privacy policy that contains specified information, including the kinds of personal information it collects, how an individual may complain about a breach of the APPs, and whether the organisation is likely to disclose information to overseas recipients. The organisation needs to take reasonable steps to make its APP privacy policy available free of charge and in an appropriate form (which will typically include making their privacy policy available on their website).

The College recommends Laboratories develop their own Privacy Policy and Information Brochure for patients and referring doctors.

APP 2 – Anonymity and Pseudonymity

This principle sets out health service providers' obligation to provide individuals with the option of dealing either anonymously or using a pseudonym.

Both requirements are subject to certain limited exceptions, including where it is impracticable for the organisation to deal with an individual who has not identified themselves, or where the law or a court/tribunal order requires or authorises the organisation to deal with individuals who have identified themselves.

The College is of the view that while an individual may have a test using a pseudonym or anonymously, this can be dangerous. An individual choosing to do this must be aware of the potential consequences, which includes:

- diagnosis and advice may be seriously impaired with consequent adverse medical outcomes;
- there may be a mismatching of the individual's results;

- there must be an acceptance that there is a consequent limitation to the liability of the pathology practice;
- it may result in breakdown in good public health practice; and
- it can not be claimed under Medicare.

Part 2 – Collection of Personal Information

APP 3 – Collection of Solicited Personal Information

This principle outlines when and how health service providers may collect personal and sensitive information that it solicits from an individual or another entity. Personal information (other than sensitive information) must not be collected unless the information is reasonably necessary for one or more of the organisation's functions or activities.

Unless an exception applies, sensitive information must only be collected with an individual's consent and if the collection is also reasonably necessary for one or more of the organisation's functions or activities. Personal information must only be collected from the individual, unless it is unreasonable or impracticable to do so. Where the patient has consented, it may be appropriate for health service providers to collect information about a patient from another medical practitioner who has also treated that patient.

Pathology laboratories collect information to:

- Link pathology reports to individuals and their health care providers
- Ensure appropriate testing
- Make a diagnosis and interpret results
- Seek confirmation or to fulfil testing requirements from third parties where appropriate
- Have available for future reference in determining trends or significant changes
- Allow billing and payments
- Fulfil regulatory and public health requirements
- Assure quality and improve processes
- For education and research purposes

Principles that set out a health service provider's obligations when collecting health information include:

1. Only collect personal health information with consent, except in specified circumstances.

   Consent to Collect or Disclose Information may be Express or Implied
   The Privacy Act states that consent may be 'express or implied'.

   Expressed consent - refers to consent that is clearly and unmistakably stated, and can be obtained either in writing, orally, or in any other form where the consent is clearly communicated.

   As a general rule, if a health service provider needs or wants consent and is in doubt about whether an individual is giving consent or not, it is preferable to seek express consent.

   Implied consent - there are situations when health service providers may reasonably rely on implied consent by individuals to handle health information in certain ways.

   For example, an individual consults a medical practitioner, discloses health information, and this is written down by the practitioner during the consultation - this will generally be

regarded as giving implied consent to the practitioner to collect the information for certain purposes. The extent of these purposes will usually be evident from the discussion during the consultation.

Similarly, if a medical practitioner collects a specimen to send to a pathology laboratory for testing, it would be reasonable to consider that the individual is giving implied consent to the passing of necessary information to that laboratory.

The Guidelines on Privacy in the Private Health Sector state *"where specialists (such as pathologists) collect information from a referring health service provider and do not personally see the individual, it may often be the case that the referring provider has gained consent (whether express or implied) to the disclosure of the information to the specialist, and to the collection by that specialist for the purposes of the referral"*.

Consent on behalf of an individual

An individual cannot give valid consent if they lack the capacity to make an informed decision. An individual may be unable to give consent for a number of reasons, including because they:

- have limited decision-making capacity due to a cognitive impairment, such as dementia or a severe intellectual disability;
- are experiencing a temporary incapacity, perhaps during a psychotic episode, due to a temporary psychiatric illness, or because of severe distress;
- are a young child; or
- are in an emergency situation and are unconscious or in distress.

A lack of decision-making capacity and privacy-related consent issues should not mean that individuals miss out on getting necessary health care, support and other services. Yet, neither should an individual's privacy rights be undermined unnecessarily by virtue of their inability to give consent.

When consent is required, and an individual lacks capacity, a health service provider may need to consider who can provide consent on the individual's behalf. There may be a range of options, including:

- a guardian;
- someone with an enduring power of attorney that can be used in relation to the individual's health;
- a person recognised by other relevant laws, for example in NSW, a 'person responsible' under the NSW Guardianship Act (this may be an individual's spouse, partner, carer, family member or close friend); or
- a person who has been nominated in writing by the individual while they were capable of giving consent.

Collection Without Consent

In situations where there is no one available to act for an individual, the health service provider may have to make decisions about appropriate handling of the individual's health information. Professional and ethical obligations and current accepted practices may provide guidance in these circumstances.

There are a limited number of situations that allow a health service provider to collect information without an individual's consent. These include where:

- there are professional rules of confidentiality of competent Health or Medical Boards which are binding and where the collection is necessary to provide a health service and is carried out according to these rules;
- there are laws requiring collection;
- there is a serious or imminent threat to life;
- information is required for management, research or statistical purposes relevant to public health or public safety, or for the management, funding or monitoring of a health service where it is impracticable to gain consent and de-identified information would not be sufficient.

The Australian Information Commissioner has also indicated that taking medical history as it relates to family members is one area where it is allowable to collect information relating to an individual (i.e. the family member) without the express consent of that individual.

Reasonable steps must be taken to ensure that individuals are aware of certain matters including, but not limited to, who is collecting the information, the fact that the individual is able to gain access to the information and the purposes for which the information is collected.

"Tip for compliance"

In the routine process of laboratory testing, pathologists do not collect information directly from individuals, however the pathologist could ensure the individual is aware of how their information will be handled via the referring provider. Alternatively, the pathologist may decide to include this information with their bill or with their report from the referral.

Only collect information necessary for the performance of the health service provider's functions or activities. In assessing what is 'necessary', professional practice standards and obligations will be relevant.

Collect information directly from the individual where this is reasonable and practicable. When collecting health information from another source (other than from the individual) APP 3 still applies. This means that either the individual has consented to the indirect collection or collection without consent is allowable under APP 3. There are a number of situations where collecting health information directly from the individual may not be reasonable or practical, for example where a pathologist collects a specimen and accompanying information from a referring provider.

APP 4 – Dealing with unsolicited Personal Information

Where health service providers receive unsolicited personal information, it must determine whether it would have been permitted to collect the information under APP 3. If so, APPs 5 to 13 apply to that information.

If the information could not have been collected under APP 3, and the information is not contained in a Commonwealth record, the organisation must destroy or de-identify that information as soon as practicable, but only if it is lawful and reasonable to do so.

APP5 – Notification of the Collection of Personal Information

Health service providers are required to take reasonable steps to inform individuals of certain matters at or before the time (or, if that is not practicable, as soon as practicable after) the

collection of personal information either directly (i.e. from the individual) or indirectly (i.e. from someone other than the individual to whom it relates). These matters are:

- the identity of the organisation and how to contact it;
- access, correction and complaints processes in its APP privacy policy;
- the purposes for which the information is collected;
- the organisations (or the types of organisations) to which the organisation usually discloses information of that kind;
- any law that requires the particular information to be collected;
- the main consequences (if any) for the individual if all or part of the information is not provided; and
- the location of any likely overseas recipients of individuals' information.

Part 3 – Dealing with Personal Information

APP 6 – Use or Disclosure of Personal Information

This principle outlines the circumstances in which health service providers may use or disclose the personal information that it holds about an individual. Specifically in Pathology:

- information is used within the laboratory for producing results and advice and delivering these to specified health providers;
- in the routine pathology process, health information may be disclosed to another provider for the purposes of getting a second opinion or where the test is a special one, the test (with the associated information) may be referred to another more appropriate laboratory;
- in very rare instances this may be outside of Australia in which case privacy must continue to be protected;
- there are some statutory requirements for reporting test results to registries;
- information is used for billing; and
- information may be used for Quality Assurance, Education or Research purposes.

Principles that set out a health service provider's obligations when using and disclosing personal information include:

1. Only use or disclose personal information for the primary purpose for which it was collected, or for directly related secondary purposes if these fall within the reasonable expectations of the individual, unless another exception under this principle applies.

   This is clarified further in the following points.

   - Sharing information with other health service providers: primary purpose, directly related secondary purposes

   The multi-disciplinary team approach to health care is common to the Australian health system. Under this approach practitioners work together and share necessary information, usually in accordance with codes of practice, to deliver optimum patient care.

   Health service providers involved in care and treatment for the **primary purpose** and/or **directly related secondary purposes** would usually not need to seek further consent for necessary uses and disclosures. This will, however, depend on the circumstances of the case and the needs and wishes of the individual.

For example, an individual goes into hospital for an operation. Generally, uses or disclosures necessary to carry out the operation (including, information sharing with pathologists, radiologists or anaesthetists) are integral in delivering the health service. Further consent is not needed where the individual reasonably expects this approach.

Other examples of necessary information sharing, which would usually fall within reasonable expectations are:

- after an individual agrees to see a specialist, necessary information sharing between the general practitioner and the specialist;
- review of specimens by a senior pathologist on request from a junior pathologist to determine a diagnosis; and
- wards rounds and team-based case reviews.

Some individuals want or need to use health services in specific ways. For instance, someone may seek care and treatment through a particular health service provider, wanting to tell certain information only to that provider. Therefore, it is likely there will be circumstances where a health service provider needs to seek consent before sharing information with another provider. This may include some second opinions.

When collecting information, it may be advisable to discuss with the individual how the team-based approach to treatment will affect the handling of personal information.

2. Other directly related secondary purposes in the health sector where consent is not required.

   Directly related secondary purposes may include many activities or processes necessary to the functioning of the health sector.

   Where the use or disclosure of de-identified data will not suffice, and provided it is within the reasonable expectations of the individual, no extra steps need be taken when using or disclosing relevant personal information in circumstances, such as:
   - providing an individual with further information about treatment options;
   - billing or debt-recovery;
   - an organisation's management, funding, service-monitoring, complaint-handling, planning, evaluation and accreditation activities - for example, activities to assess the cost effectiveness of a particular treatment or service;
   - disclosure to a medical expert (only for medico-legal opinion), insurer, medical defence organisation, or lawyer, solely for the purpose of addressing liability indemnity arrangements, for example in reporting an adverse incident;
   - disclosure to a lawyer for the defence of anticipated or existing legal proceedings;
   - an organisation's quality assurance or clinical audit activities, where they evaluate and seek to improve the delivery of a particular treatment or service; and
   - disclosure to a clinical supervisor by a psychiatrist, psychologist or social worker.

3. Only use or disclose personal information in other ways if the individual gives consent (whether express or implied), or if one of the exceptions to this principle applies. The exceptions include, but are not limited to, uses or disclosures required or authorised by law, those necessary to prevent or lessen a serious or imminent threat to someone's life, health or safety, or for research provided certain conditions are met.

- Uses and Disclosures with Consent

A health service provider can use or disclose personal information for almost any purpose if they have the consent of the individual.

(a) Training and Education

It is important for health service providers to be able to train in 'real life' environments. Training and education, in some cases, may be as effective by using de-identified case studies, or in the case of IT training through using simulated data. If a health service provider uses de-identified information for training, consent is not required.

Where the use of health information is necessary for training purposes, the sensitivity of such information needs recognition as some individuals seeking health care may not want their information disclosed any more widely than is necessary to receive care. These individuals may not want their information used for training or education activities.

The use of information for training and education will therefore usually require the individual's consent.

"Tips for compliance"
Whether consent is needed may depend on the nature of the training activity and the expectations and wishes of the individuals involved.

Intrusive training activities, or those less closely linked with service provision, are more likely to require express consent. For instance, videotaping a family therapy session, when the identities of participants will be revealed, is highly likely to require express consent.

Where consent is sought, the individual should have a genuine choice and not be pressured to participate. The individual should be told about the specific nature of the activity and the student group involved.

(b) Transferring records to another health service provider on request.

If an individual wants to transfer their care to another health service provider, they can authorise the disclosure of health information from the original provider to the new provider. A copy of this information could be transferred in this way.

However, if the original provider declines to transfer the information, then under APP 12 the individual may request access to the health information and seek a copy. Unless an exception under APP 12 applies, the provider is obliged to give a copy of the record to the individual, who can then take it to the new health service provider.

(c) Other areas where consent is generally required before a health service provider can disclose personal information include:
- Media;
- Fundraising; and
- Direct Marketing.

4. APP 6 also deals with other matters, including when a health service provider can disclose health information to a 'person responsible' for an individual who cannot give or communicate their consent.

5. Finally, there are a number of areas where use and disclosure may occur without the individual's consent:

   - Use and disclosure necessary for research and statistics relevant to public health or public safety

     In limited circumstances, this provision allows uses or disclosures of health information for research purposes, or for the compilation or analysis of statistics without consent, where these activities are relevant to public health or public safety. That is, the research must be about, or the statistics related to, public health or safety.

     Health information may be used or disclosed without consent for these purposes, only if:

     - the activities are relevant to public health and safety;
     - seeking consent is impracticable;
     - the activities are carried out in accordance with guidelines that are developed by the National Health and Medical Research Council (or a prescribed authority) and are approved by the Australian Information Commissioner; and
     - for disclosure - the health service provider reasonably believes that the organisation to which they disclose will not further disclose the health information or any personal information derived from it.

     When deciding whether a use or disclosure is 'necessary' for research or statistics, a health service provider must consider whether employing de-identified information would be sufficient. If de-identified information would suffice, the provider cannot use this principle to justify using identified information.

     Whether it is impracticable to seek consent will depend on the particular circumstances of the case. Simply incurring some expense, or having to exercise some effort to seek the consent of individuals whose information is to be used or disclosed, would not ordinarily make it 'impracticable' to seek consent. Circumstances where it may be impracticable to seek consent could include where there are no current contact details for the individuals in question and where there is insufficient information to get up-to-date contact details. This might occur in longitudinal studies of old records.

   - Serious threats to life, health or safety

     In limited circumstances, a health service provider may need to use or disclose personal information to lessen or prevent:
     - a serious and imminent threat to an individual's life, health or safety; or
     - a serious threat to public health or public safety.

     This exception allows for such uses and disclosures and generally relates to emergencies. Depending on the circumstances, this exception can allow disclosures to the police service or other government authorities, such as a community services department or mental health crisis team. The exception also allows for disclosure to an individual whose life, health or safety is threatened.

A 'serious and imminent' threat to an individual's life, health or safety relates to harm that could be done to any person (including the individual seeking treatment and care).

A 'serious' threat must reflect significant danger, and could include a potentially life threatening situation or one that might reasonably result in other serious injury or illness. Alternatively, it could include the threat of infecting a person with a disease that may result in death or disability. A threat could also relate to an emergency, following an accident, when an individual's life or health would be in danger without timely decision and action.

A threat is 'imminent' if it is about to occur. This test could also include a threat posed that may result in harm within a few days or weeks. It is much less likely to apply to situations where the risk may not eventuate for some months or longer.

A 'serious' threat to public health or public safety relates to broader safety concerns affecting a number of people. This could include the potential spread of a communicable disease, harm caused by an environmental disaster or harm to a group of people due to a serious, but unspecified, threat.

- Use and disclosure regarding suspected unlawful activity

  This provision recognises the legitimate function of an organisation, including a health service provider, in investigating (internally) and reporting suspected unlawful activity. Usually, but not in all cases, the suspected unlawful activity would relate to the operations of the health service provider.

  Such investigations may include the internal handling of complaints or allegations regarding professional misconduct, sexual harassment or assault and the reporting of them to the police or another relevant person or authority.

- Use or disclosure required or authorised by law

  The Privacy Act recognises other legal obligations to use or disclose personal information. 'Law' in this context includes Commonwealth, State and Territory legislation, and the common law.

  If the law requires that a health service provider use or disclose information, the provider must do so. Examples of such requirements include the mandatory reporting of child abuse (under care and protection laws) or the notification of diagnoses of certain communicable diseases (under public health laws).

  Disclosure must occur if there is a warrant or law requiring the health service provider to do so.

APP 7 – Direct Marketing

Generally, health service providers may only use or disclose personal information for direct marketing purposes where the individual has either consented to their personal information being used for direct marketing, or has a reasonable expectation that their personal information will be used for this purpose, and conditions relating to opt-out mechanisms are met. Health service providers may not use sensitive information (including health information) for direct marketing unless the individual has consented to that use of disclosure.

This principle permits contracted service providers for Commonwealth contracts to use or disclose personal information for the purpose of direct marketing if certain conditions are met.

APP 8 – Cross-Border Disclosures

Before disclosing personal information to an overseas recipient, health service providers are required to take reasonable steps to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to that information. In some circumstances an act done, or a practice engaged in, by the overseas recipient that would breach the APPs, is taken to be a breach of the APP's by the referring health service provider. There are a number of exceptions to these requirements.

APP 9 - Adoption, Use or Disclosure of Government Related Identifiers

This principle sets out health service providers obligations when handling Government related identifiers such as Medicare numbers. Health service providers must not use or disclose a government related identifier of an individual, or use a government related identifier of an individual as the organisation's own identifier of the individual, unless an exception applies.

APP10 – Quality of Personal Information

Health service providers are required to take reasonable steps to ensure the personal information collected by the organisation is accurate, up-to-date and complete.

For uses and disclosures, the personal information must be relevant, as well as, accurate, up-to-date and complete, having regard to the purpose of the use or disclosure.

APP11 – Security of Personal Information

Health service providers are required to take reasonable steps to protect the personal information they holds from interference, in addition to misuse and loss, and unauthorised access, modification and disclosure. Health service providers are also required to take reasonable steps to destroy or de-identify personal information if the organisation no longer needs it for any authorised purpose. There are two exceptions to this requirement:

- the personal information is contained in a Commonwealth record; or
- the organisation is required by or under an Australian law or a court/tribunal order to retain the information.

APP 12 – Access to Personal Information

Health service providers are required to give an individual access to the personal information that they hold about that individual, unless an exception applies. Health Service providers are further required to respond to requests for access within a reasonable period (usually 30 days). In addition, access must be given in the manner requested by the individual if it is reasonable to do so.

If an individual access is denied to their personal information, the health service provider must generally provide written reasons for the refusal and the mechanisms available to complain about the refusal. If an individual is charged for receiving access to the individual's personal information, the charge must not be excessive, and must not apply to the making of the request.

Please refer to RCPA Guideline for *Release of Pathology Results to Patients*, 2/2001. The preferred way for patients to receive pathology results is in a consultation with their referring doctor, where results can be explained in the context of their health management. Individuals do, however, have the right of access to their pathology records. To protect the privacy of the individual, health service providers should ensure that they properly verify the identity of the requesting individual before disclosing pathology records.

The Australia Privacy Principles state that while an individual must not be charged for lodging a request for access, a Practice may recover administrative costs for photocopying, staff time and other costs incurred by the health service provider in granting the access. Such charges must not be excessive and should not discourage an individual from accessing their records.

APP 13 – Correction of Personal Information

Health service providers are required to take reasonable steps to correct personal information to ensure that, having regard to a purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading, if either:

• the organisation is satisfied that it needs to be corrected, or
• an individual requests that their personal information be corrected.

Health service providers need to notify other entities that have been provided with the personal information of any correction, if that notification is requested by the individual.

Health service providers must also respond to a correction request (or a request to associate a statement by the individual disputing the accuracy of the information if the organisation does not agree to the correction request) within a reasonable period after the request is made, and must not charge the individual for making the request, for correcting the personal information, or for associating the statement with the personal information.

When refusing an individual's correction request, the organisation must generally provide the individual with written reasons for the refusal and notify them of available complaint mechanisms.

Mandatory Notification of Data Breaches

Under the new Notifiable Data Breach (NDB) scheme, health service providers have data breach notification obligations when a data breach is likely to result in serious harm to any individuals whose personal information is involved in the breach. This applies to all kinds of personal and sensitive information. Examples include names, addresses, email addresses, genders, family members, and medical history. When information of these types is collected and stored, steps must be taken to keep it secure and safe and to avoid loss or unauthorised access or disclosure.

What type of breaches are 'notifiable?

Health service providers have an obligation to notify affected individuals if an 'eligible data breach'. An eligible data breach occurs if all the following apply:

1. There is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information (such as infiltration by hackers or by accidentally emailing personal information to the wrong recipient) or a loss of personal information (such as unauthorised access or disclosure because of the loss of unsecured mobile device containing personal information).

2. The incident is likely to result in serious harm to individuals. 'Serious harm' could include risks to personal safety, damage to reputation, or serious psychological harm.
3. The health service provider has not been able to prevent the likelihood of serious harm by taking remedial action (such as retrieving the lost mobile device).

The NDB scheme only applies to eligible data breaches that occur from 22 February 2018.

Examples of Data Breach

A data breach can occur due to a cyber-attack, loss or theft of a device that contains personal information, or because personal information that gets published or shared without authorisation (whether deliberately or inadvertently). Examples may include when any electronic or cloud-based database containing medical records is hacked, health information is mistakenly provided to the wrong person (for example, via email) or an electronic device containing patients' medical records is lost or stolen.

If unsure, medical practitioners and other health service providers can seek advice from their medical defence organisation before taking any further actions to proceed. However, advice must be sough urgently so that the health service provider can comply with any notification obligations.

What must Health care providers do if data has been breached?

If a health service provider suspects or knows that a data breach has occurred, the health service provider must promptly investigate the breach to determine whether it is an eligible data breach. An eligible data breach will have occurred if the data breach like to result in serious harm. The health service provider must take all reasonable steps to complete the investigation within thirty days of the date on which health service provider first suspects that there might have been a data breach.

Notification must occur as soon as the health service provider believes that eligible data breach has occurred. If a notifiable breach has occurred, report details of it to the individual, and to the OAIC (Office of the Australian Information Commissioner). The police may also need to be notified if a crime is suspected. The notification should set out:

- the identity and contact details of the health service provider;
- a description of the data breach;
- the kind of information involved in the data breach; and
- recommendations about the steps that the individual should take in response to the data breach. If health service providers are unable to notify the individual personally (via email or phone for instance), then a notification should be published on the health service provider's website and publicly via other channels such as the media.

The investigation period of thirty days is a short window of time, as the investigation of data breaches can be complex, time-consuming and expensive. It is therefore important that health service providers have procedures in place for dealing with a data breach when a data breach occurs.

Health service providers should strengthen internal procedures and systems to reduce the risk of regulatory penalties, financial losses, damaged reputation, and loss of patient trust. This includes using appropriate and up-to-date technology to increase data security, to ensure compliance and prevent potential breaches. This can include more robust methods of encryption, regular and secure backups, restricted access, and password controls for any patient information.

One or more staff members should be allocated the responsibility for overseeing information management, mitigation and risk, and for investigating any actual or suspected data breaches.

Change in business circumstance or closure of health service

An area which is likely to affect the operation of pathology practices is the impact the privacy provisions have on a change in business circumstance or closure of a health service.

A health service provider's business circumstances could change in a number of ways. A provider may amalgamate with other providers or businesses, another business may take over the existing provider's practice, the provider may close down, or the services may cease because the health service provider (if they are a sole practitioner) retires or dies. The following principles apply if there is a change in business circumstance:

1. Information stays with the original health service provider organisation

   In some cases, the nature or ownership of a health service provider changes, but the legal entity or organisation remains in existence. Here, the APPs do not require any additional action unless the organisation is proposing to change the purposes for which it uses or discloses personal information. The new purposes would need to be addressed in ways consistent with the provisions of APP 6 *Use and Disclosure of Personal Information.*

   If the health service provider uses an individual's health information as it did before, in providing health care, then there is no requirement to inform, or seek consent from, the individual.

   However, if as a result of the change, the health service provider intends to use the information for purposes that are not consistent with the primary purpose of collection, or are not directly related secondary purposes and within the reasonable expectations of the individual, then the provider may need to seek consent.

   For example, a general practice expands, creating a medical centre with same-provider pathology, radiology, counselling and other services.

   The provider wants all patient health information to be available to all their health professionals, some of whose services have no direct relation to the reasons the individual consults the general practitioner. As some of these uses may fall outside the individual's reasonable expectations, APP 6 may require that consent be sought, unless one of the exceptions to the principle applies.

2. Information is moved to a new health service provider

   In circumstances where there is a new legal entity, for example in some takeovers or mergers, there may be a transfer of personal information. Under the APPs this means there will be a disclosure by the old organisation and collection and use by the new organisation.

   For example, when a health service provider closes, selling their operations to a wholly new provider, the new provider will take over their assets and patient-base (including databases).

   (a) Disclosure by the old health service provider

The APPs permit disclosure of health information without further obligations where this is for the primary purpose for which the information was collected, or where the disclosure is directly related to the primary purpose and within the individual's reasonable expectations.

The old health service provider and the new provider will need to work together to determine whether the transfer of personal information (including sensitive information) would be permissible under the APPs. Generally speaking, if the new provider will continue to conduct the same or very similar business, disclosure may be permitted upon the transfer of the other business assets of the old provider to the new provider. If necessary, separate legal advice should be sought on this issue.

Where there is doubt about whether disclosures would fall within the scope of the permitted disclosure, the safer course would be to obtain consent before disclosing health information.

(b) Collection and use by the new organisation

Ordinarily, the new health service provider will need consent before collecting individuals' health information, unless one of the exceptions to APP 3 applies. The provider may also need to tell the individuals that it now holds information about them, give its contact details and other information.

The old and the new health service providers may decide between them how to handle these obligations.

If an individual does not consent to the transfer of their information, they may wish to have it transferred to another health service provider.

3. A health service provider's business ceases

Where a health service provider ceases operations and no other provider is taking over, arrangements will need to be made for the appropriate storage and transfer of individuals' health information. This situation might occur where a health service provider retires or dies.

Generally, the destruction of health information in this circumstance is not good practice. Destruction may also be inconsistent with other laws or regulations.

In the event that the health information is to be transferred to another health service provider, then consent for disclosure and collection may need to be obtained (see the discussion above).

Where individuals cannot be contacted, appropriate arrangements may need to be made to secure the data for future access by those individuals, or for other permitted uses and disclosures.