NATIONAL PATHOLOGY ACCREDITATION ADVISORY COUNCIL

REQUIREMENTS FOR INFORMATION COMMUNICATION

(Third Edition 2013)

NPAAC Tier 3B Document

Print ISBN: 978-1-74241-919-0

Online ISBN: 978-1-74241-920-6

Publications approval number: 10207

Paper-based publications

Internet sites

First published 1998
Second edition 2007 reprinted with revisions and name change from *Guidelines for Data Communication*
Third edition 2013 reprinted and reformatted to be read in conjunction with the *Requirements for Medical Pathology Services*

Australian Government Department of Health

Contents

Scope v

Abbreviations vi

Definitions vii

Introduction 1

1. Privacy principles 5

Collection of information 6

Use and disclosure of information 7

Data quality and correction of data 9

Data security and data retention 10

Openness and access 12

Use of identifiers and anonymity 14

Inter-jurisdictional data flows 15

Transfer or closure of the Laboratory 15

2. Documentation 16

3. Security of storage 17

4. Security of data management (including access) 18

5. Security of messaging 19

6. Compliance with electronic messaging standards 21

7. Business continuity planning (including archiving) 22

8. Laboratory audit trail 23

Appendix A Online versions of national, state and territory privacy legislation (Informative) 25

Bibliography 27

Further information 28

The National Pathology Accreditation Advisory Council (NPAAC) was established in 1979 to consider and make recommendations to the Australian, state and territory governments on matters related to the accreditation of pathology laboratories and the introduction and maintenance of uniform standards of practice in pathology laboratories throughout Australia. A function of NPAAC is to formulate Standards and initiate and promote education programs about pathology tests.

Publications produced by NPAAC are issued as accreditation material to provide guidance to laboratories and accrediting agencies about minimum Standards considered acceptable for good laboratory practice.

Failure to meet these minimum Standards may pose a risk to public health and patient safety.

Scope

The *Requirements for Information Communication* is a Tier 3B NPAAC document and must be read in conjunction with the Tier 2 document *Requirements for Medical Pathology Services*. The latter is the overarching document broadly outlining standards for good medical pathology practice where the primary consideration is patient welfare, and where the needs and expectations of patients, Laboratory staff and referrers (both for pathology requests and inter-Laboratory referrals) are safely and satisfactorily met in a timely manner.

Whilst there must be adherence to all the Requirements in the Tier 2 document, reference to specific Standards in that document are provided for assistance under the headings in this document.

This document covers the communication of pathology information between pathology requesters, consumers and Laboratories. It emphasises the role of the Laboratory and defines the boundary of responsibility of the Laboratory and its processes.

Throughout these Requirements, practices considered desirable to improve safety, security and privacy, consistent with best practice, have been identified within Standards and Commentary. However, a Laboratory may be limited in its ability to influence requesting doctors to implement desirable practices.

Abbreviations

AS	Australian Standard
ISO	International Organization for Standardization
NPAAC	National Pathology Accreditation Advisory Council

Definitions

Access audit trail	means a record of views of an individual's health record data without modification by people, recording (as a minimum) date, time, patient identifier and person viewing. Access to data performed regularly as part of routine operations may be recorded to a lower degree of specificity. (see also 'audit trail')
Aggregated data	means data about a collection of patients, which by its nature makes the identification of individuals difficult.
Audit trail	means a chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function.
Authentication	means the process that verifies the claimed identity of a station, originator or individual as established by an identification process. Authentication ensures that the individual or organisation is who they claim to be. Comment: Authentication of the origin of a message received from an alleged sender may be by means of direct telephone dial, virtual private network with password or with digital certificates (secure socket layer [SSL], or public key infrastructure [PKI]).
Clinical acknowledgment	means a record of acknowledgment that a clinician has received and is taking responsibility for acting on results; this may be delivered by any means including phone, and clinical application acknowledgement.
Clinical application acknowledgment	means a computer generated acknowledgment by the receiving clinical application confirming receipt and processing of data.
Edit audit trail	means a record of additions and alterations to an individual's health record, including (as a minimum) date, time, patient identifier, instrument and/or authorising person, and the nature of the edit.
Electronic report	means a report message transmitted using computer.
Electronic request	means a request message transmitted using computer.

Referral	means a request plus Specimen or patient. Comment: For purposes of this document, a referral constitutes a request accompanied by a Specimen. For instance, (1) a consumer presents at a collection centre with a request form from a practitioner; or (2) a Specimen plus referral form is received by a Laboratory from a surgery. A request per se does not constitute a referral, and a Laboratory has no control over whether, in case (1), the consumer presents for Specimen collection, or to which Laboratory they may present. In case (2), the Laboratory cannot determine the forwarding of collected Specimens together with requisite request forms.
Request	means a requisition received to perform a test on a patient without the physical presence of a patient or Specimen. It can be paper or electronic.
Requirements for Medical Pathology Services (RMPS)	means the overarching document broadly outlining standards for good medical pathology practice where the primary consideration is patient welfare, and where the needs and expectations of patients, Laboratory staff and referrers (both for pathology requests and inter-Laboratory referrals) are safely and satisfactorily met in a timely manner. The standard headings are set out below – Standard 1 – Ethical Practice Standard 2 – Governance Standard 3 – Quality Management Standard 4 – Personnel Standard 5 – Facilities and Equipment A – Premises B – Equipment Standard 6 – Request-Test-Report Cycle A – Pre-Analytical B – Analytical C – Post-Analytical Standard 7 – Quality Assurance
Third-party access	means access by a party other than the original requester or original ‘copy to’ party; usually this would be a hospital, specialist or a new general practitioner.

Third-party enquiry	means a request by an entity other than the original requesting authority for a copy of a report(s). This is considered a 'directly related secondary purpose'.
Transport acknowledgment	means a computer or machine generated acknowledgment confirming delivery of a message to a location; this ensures, to a reasonable degree of certainty, that a message has been successfully delivered, but does not ensure that a clinician has taken appropriate and timely responsibility to act; this applies equally to electronic messages and facsimile transmissions (a facsimile transmission is not deemed successful until a transport acknowledgment is received).
Urgent	means 'Requiring immediate attention' as determined by the requesting practitioner or by the Laboratory (Concise Oxford Australian Dictionary 1997).

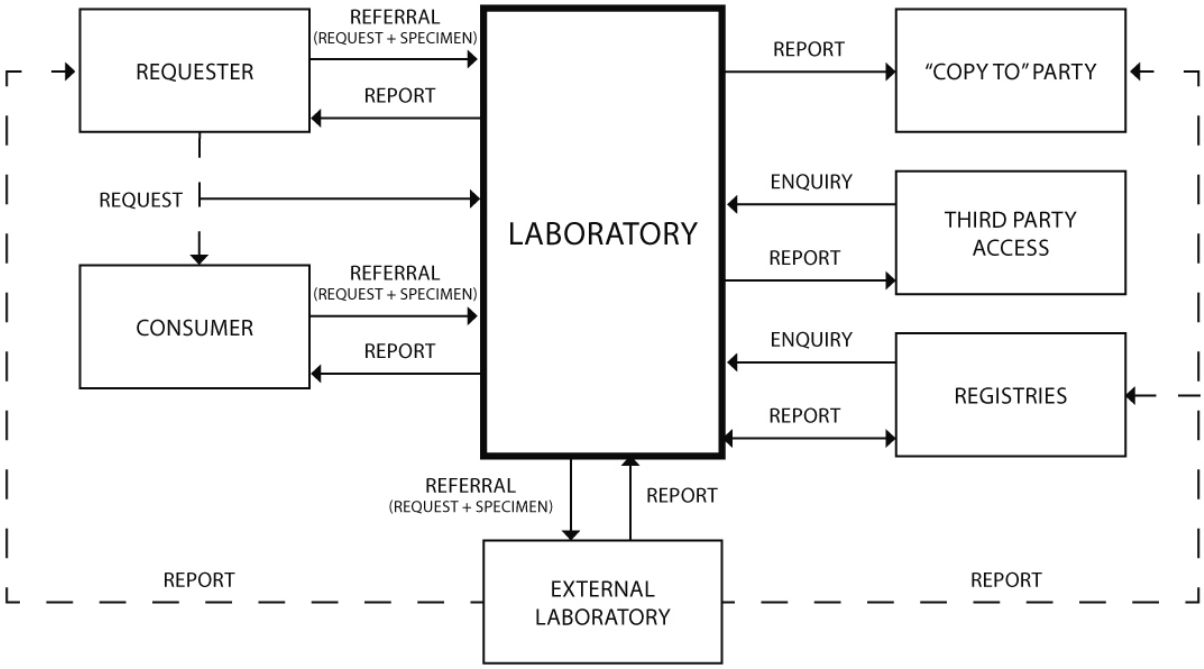
This page is intentionally blank

Introduction

The integration of computer systems and telecommunications offers faster transfer of pathology requests and reports. However, there is a need to consider privacy and data protection principles and to ensure the correct transmission and receipt of reports. NPAAC's statutory role in the regulation of Laboratories makes it the logical body to formulate Standards for the way pathology data is communicated. However, these Standards are not intended to replace other requirements that may be imposed under Commonwealth or state or territory laws, or by institutional ethics review committees.

Laboratory responsibilities are confined to activities within the Laboratory and where there is interaction with external bodies, as described in Figure 1.

Figure 1 Laboratory messaging in context



The Laboratory is responsible for acting when:

- a request and Specimen is collected from a requester or delivered to the Laboratory
- a request is received from a requester via a consumer (e.g. presentation of patient with request form at collection centre)
- an enquiry is received from a third party
- a request is received for additional testing on an existing Specimen.

The Laboratory is considered to have fulfilled its responsibility when:

- for routine reports, a result has been sent and a transport acknowledgment has been received (delivery of result by electronic means only)
- for urgent reports, a result has been sent and there has been clinical acknowledgment, or clinical application acknowledgment. That is, it is certain the requesting practitioner or proxy has received it (any mode of communication)
- for 'amended final report', if there is variation in the result that is clinically significant, the Laboratory has treated the amended final report as an urgent report.

An electronic request which is yet to become a referral is outside the scope of this document.

Several methods of pathology communication can be identified for requests, reports, and inter-Laboratory and intra-Laboratory communication, including:

- physical delivery of paper documents, with manual data entry
- telephoning
- faxing, with manual data entry
- short messaging service (SMS) text messaging
- electronic file transfer on physical media
- remote access to the pathology system by direct dial-in or web access
- electronic messaging using standard protocols
- access via a third-party data repository (e.g. cancer registries).

To facilitate the secure and private transmission of pathology requests and reports, Laboratories must be able to ensure the confidentiality, integrity (including authenticity) and availability (collectively known as information security) of messages received and sent. This includes recording, storing and, where required, archiving messages. Each method introduces its own particular risks. Addressing these risks requires attention to information security risk management. Australian Standards AS/ISO17799 *Information Security Management* and HB174 *Information Security Management Implementation Guide for the Health Sector* provide guidance on this.

In ensuring risks are well managed, systems managers should pay particular attention to:

- manual data entry of request form information
- address (destination) requirements for transmitted information
- authentication where remote access is granted
- appropriate security during transmission and receipt.

Unique request numbers generated by requesting systems provide the most reliable method of correlating requests and reports, especially when identifying information does not match or reports do not match requests.

AS4700.2 *Implementation of Health Level Seven* recommends a method for correlating requests, Specimens, results, add-on tests, and reflex tests.

AS5017 *Health Care Client Identification* provides guidance on patient identification and data matching.

This document is issued by NPAAC for the guidance of Laboratories in Australia, providing minimum standards considered acceptable for good pathology practice in relation to the transfer of data, including electronic transfer. It should be read in conjunction with other NPAAC documents. Information communication is evolving, and Laboratory accreditation procedures may need to evolve with it.

These Requirements should be read within the national pathology accreditation framework including the current versions of the following NPAAC documents:

Tier 2 Document

- *Requirements for Medical Pathology Services*

All Tier 3 Documents

In addition to these Standards, Laboratories must comply with all relevant state and territory legislation (including any reporting requirements).

In each section of this document, points deemed important for practice are identified as either 'Standards' or 'Commentaries'.

- A Standard is the minimum requirement for a procedure, method, staffing resource or facility that is required before a Laboratory can attain accreditation — Standards are printed in bold type and prefaced with an 'S' (e.g. **S2.2)**. The use of the verb '**must**' in each Standard within this document indicates a mandatory requirement for pathology practice.
- A Commentary is provided to give clarification to the Standards as well as to provide examples and guidance on interpretation. Commentaries are prefaced with a 'C' (e.g. C1.2) and are placed where they add the most value. Commentaries may be normative or informative depending on both the content and the context of whether they are associated with a Standard or not. Note that when comments are expanding on a Standard or referring to other legislation, they assume the same status and importance as the Standards to which they are attached. Where a Commentary contains the word '**must**' then that Commentary is considered to be **normative**.

Please note that the Appendix attached to this document is **informative** and should be considered to be an integral part of this document.

Please note that all NPAAC documents can be accessed at www.health.gov.au/internet/main/publishing.nsf/Content/health-npaac-publication.htm

While this document is for use in the accreditation process, comments from users would be appreciated and can be directed to:

The Secretary
NPAAC Secretariat
Department of Health
GPO Box 9848 (MDP 951)
CANBERRA ACT 2601

Phone: +61 2 6289 4017
Fax: +61 2 6289 4028
Email: npaac@health.gov.au
Website: www.health.gov.au/npaac

1. Privacy principles

(Refer to Standard 1, Standard 2, Standard 3, Standard 4 and Standard 6 in *Requirements for Medical Pathology Services*)

Public and private pathology providers are subject to different regulatory schemes for collecting, handling, storing and transmitting patient data. Private sector pathology providers are subject to the *Commonwealth Privacy Act 1988* and may also be subject to local state or territory privacy regulations. There is also a published Australian Association of Private Pathology industry policy that should be followed. Public sector pathology providers are subject to individual state or territory regulations with the exception of those in the Australian Capital Territory, who are subject to both Commonwealth and territory regulation.

In addition, the Australian Health Ministers' Advisory Council (AHMAC) is developing a national health privacy code. The main objective of this code is to achieve consistency across the private and public sectors through a single national code for the appropriate collection and handling of health information. The standards concerning privacy in this NPAAC document are based on AHMAC's proposed national health privacy code, but Laboratories must also ensure that they comply with appropriate state, territory and Commonwealth legislation or regulations.

Standards concerning privacy principles are considered under:

- compliance with legislation
- collection of information
- use and disclosure of information
- data quality and correction of data
- data security and data retention
- openness and access
- use of identifiers and anonymity
- inter-jurisdictional data flows
- transfer or closure of the Laboratory.

Table 1 indicates the legislation and regulations that apply in each state and territory of Australia.

Table 1 Laboratory compliance with state and territory privacy legislation and regulations

State or Territory	Public sector laboratory	Private sector laboratory
Australian Capital Territory	*Privacy Act 1988 (Cwlth)* *Health Records (Privacy and Access) Act 1977*	*Privacy Act 1988 (Cwlth)* *Health Records (Privacy and Access) Act 1977*
New South Wales	*Privacy and Personal Information Protection Act 1998* *Health Records and Information Privacy Act 2002*	*Privacy Act 1988 (Cwlth)* *Health Records and Information Privacy Act 2002*
Northern Territory	*Information Act 2002*	*Privacy Act 1988 (Cwlth)*
Queensland	Information Standards 42A (Health)	*Privacy Act 1988 (Cwlth)*
South Australia	Information Privacy Principles	*Privacy Act 1988 (Cwlth)*
Tasmania	*Personal Information Protection Act 2004*	*Privacy Act 1988 (Cwlth)*
Victoria	*Information Privacy Act 2000* *Health Records Act 2001*	*Privacy Act 1988 (Cwlth)* *Health Records Act 2001*
Western Australia	*Health Act 1911*	*Privacy Act 1988 (Cwlth)*

Collection of information

S1.1 The Laboratory must only collect health information about an individual that is necessary for the Laboratory's functions and where the individual has given consent. However, there are circumstances where health information may be collected without the consent of the individual.

C1.1 Health information about an individual may be collected without the consent of that individual when the information:

(i) will provide a health service to the individual and the individual is incapable of giving consent

(ii) will prevent or lessen a serious and imminent threat to the life, health, welfare or safety of any individual

(iii) will establish or defend a legal or equitable claim

(iv) is part of a family medical history, social medical history or is other relevant information about an individual that is collected to provide a health service to a person (including the individual), and is collected by a health service provider from either the person who is to receive the service or from a relative or carer of the individual.

S1.2 Where it is reasonable and practicable to do so, health information about an individual must be collected only from that individual, or from a person who is responsible for that individual, or from the referring medical practitioner.

C1.2 Where it is not reasonable or practicable to collect health information from an individual due to age or infirmity, such information may be collected from the parent, guardian or carer of the individual.

S1.3 The Laboratory must take reasonable steps to ensure that the individual is aware of any health information collected, including tests to be performed, and that the individual can request access to such information.

C1.3 Individuals should be given the name and contact information of the Laboratory in order to access their health information.

Use and disclosure of information

S1.4 A Laboratory must not use or disclose an individual's health information, including results, except for the primary or directly related secondary purpose for which the information and/or results were collected or produced. In certain circumstances, such information may be used for non-directly related secondary purposes.

C1.4(i) Use refers to the handling of information within an organisation whereas disclosure refers to transfer of information outside the organisation.

C1.4(ii) The primary purpose is the main reason that an organisation collects or acquires health information or test results from an individual (e.g. to make a diagnosis).

C1.4(iii) A directly related secondary purpose may include activities necessary for the proper functioning of the Laboratory, and will usually be closely bound to the primary purpose (e.g. seeking of a second opinion, billing or debt recovery, disclosure to a medical defence organisation when reporting an adverse incident). Directly related secondary purposes would not normally require special circumstances for the use or disclosure of the health information.

C1.4(iv) A non-directly related secondary purpose normally requires permission from the individual for the use or disclosure of the individual's health information (e.g. staff training, health service evaluation or monitoring, use of patient databases for fundraising and/or direct marketing). In certain circumstances however, permission is not required to use or disclose an individual's health information.

C1.4(v) Health information and test results may be used for a directly related secondary purpose where the individual would reasonably expect the organisation to use or disclose the information for that purpose.

C1.4(vi) Health information and test results may be used for a non-directly related secondary purpose:

(a) where the individual has consented to the use or disclosure

(b) where the use or disclosure is required, authorised or permitted by law (e.g. reporting a notifiable disease)

(c) where the Laboratory providing a health service to an individual reasonably believes that such use or disclosure is necessary for the provision of that health service, and the individual is incapable of giving consent

(d) where the Laboratory providing a health service reasonably believes that the use or disclosure is necessary to ensure that further health services are provided safely and effectively

(e) where the use or disclosure is for the purpose of funding, management, planning, monitoring, improvement or evaluation of health services, including training of staff or other persons being trained by the organisation and where:

- the purpose cannot be achieved by using de-identified data, and it is impractical to seek the individual's consent; or
- reasonable steps are taken to de-identify the data

(f) where the Laboratory reasonably believes that the use or disclosure is necessary to lessen or prevent:

- a serious and imminent threat to an individual's life, health, safety or welfare; or
- a serious threat to public health or safety

(g) where the use or disclosure is required for research, or the compilation or analysis of statistics, in the public interest and:

- it is impractical to seek the individual's consent; and
- the purpose cannot be achieved by using de-identified data and, in the case of disclosure, it will not be published in a form that identifies individuals

(h) in the case of genetic information of an individual that is, or could be, predictive at any time of the health of another individual, and the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to that other individual's life, and:

- a reasonable attempt has been made to obtain consent from the first individual;

- it is not reasonably practicable to obtain the consent of that individual; or
- that individual is incapable of giving consent

(i) where the use or disclosure is necessary to establish, exercise or defend a legal or equitable claim

(j) where the health information is about a deceased individual and is to be used by or disclosed to:

- a legal representative of the deceased;
- a person who was the authorised representative of the deceased and the disclosure is for a purpose relating to the former powers, functions or duties of that person;

C1.4(vii) De-identified health information is information that does not identify an individual, and where there is no reasonable basis to believe that the information can be used to identify an individual. The size of a specific population will affect the criteria determining which data must be removed to ensure that an individual cannot be identified from published de-identified data (e.g. postcodes of small communities, age [year of birth] where individuals are over the age of 89). Methods that may be used to de-identify data include the safe harbour method and the statistical method. Laboratories should be aware that privacy principles may still apply to de-identified information depending on what other knowledge the recipient has. These data may be referred to as 'aggregated data'.

C1.4(viii) Where possible, individuals should be made aware of any persons or organisations (in addition to the referring practitioner) to whom their health information, including results, may be disclosed (e.g. cancer or cervical registries). Where the Laboratory has disclosed, or intends to disclose, health information to a registry or other pertinent body, the Laboratory may indicate this in the test result report.

Data quality and correction of data

S1.5 The Laboratory must take all reasonable steps to ensure that the health information that it collects, produces, uses or discloses is accurate, complete and up-to-date, and relevant to its functions and activities.

C1.5 Some factors to consider in determining 'reasonable steps' are the likelihood that the information is complete, accurate and up-to-date; whether the information can change over time (e.g. address, date of birth); how recently that information was collected; who provided the information and how the information will be used.

S1.6 If a Laboratory holds health information about an individual and the individual is able to establish that the information is inaccurate, incomplete, misleading or not up-to-date, the Laboratory must incorporate the correct information into the health record.

C1.6(i) The Laboratory should develop protocols for dealing with the changing status of confidence in Laboratory data where new knowledge and technology have resulted in significant change in the quality and clinical interpretation of Laboratory data.

C1.6(ii) Where an individual requests a significant change to his or her stored health information, there may be important medical and legal reasons for retaining a complete record. Consequently, the requested changes should be appended, but the original information should also be retained in the record.

Data security and data retention

S1.7 The Laboratory must take reasonable steps to protect the information it holds from misuse, loss, and from unauthorised access, modification or disclosure.

C1.7(i) Access to health records should be protected by robust password control and regular changes of passwords.

C1.7(ii) Data security should be part of the organisation's data management policy that includes retention, storage and disposal of health information. It should also include management of electronic and physical aspects, with steps taken to protect against intentional and inadvertent loss and/or breach.

C1.7(iii) Surplus personal computers and other media storage devices should be retired or disposed of in such a way as to ensure that health information that may have resided on them can no longer be accessed.

C1.7(iv) Computer screens and fax machines should be positioned so that they cannot be seen by unauthorised people (e.g. members of the public).

S1.8 The Laboratory must retain (and therefore must not delete or destroy) health information relating to an individual, even if it is later found or claimed to be inaccurate, unless the deletion or destruction is permitted or required by law.

S1.9 The Laboratory must retain records according to the requirements given in the appropriate NPAAC document addressing the retention of records and as required by relevant legislation.

C1.9(i) Given the relative ease with which large amounts of data can now be electronically stored and retrieved, Laboratories are encouraged (in the interests of patient care, future epidemiology and research) to consider long-term retention and secure storage of Laboratory data beyond the mandated requirements in standard **S1.10**.

C1.9(ii) The retention of records relates to both data that are used solely by the Laboratory and those that are communicated to other organisations or individuals. Patient health information must be kept for at least seven years from the date of the last entry in the record. However, if the patient was less than 18 years old at the date of the last entry in the record, the record must be kept until the patient attains or would have attained 25 years of age.

C1.9(iii) The Laboratory may choose to retain health records, even though deletion or destruction is permitted under standards **S1.9** and **S1.10**, where those records are needed for either the primary purpose or any secondary purpose permitted under these Standards.

C1.9(iv) The Laboratory should have a records management policy incorporating data management and protocols relating to retention, storage and disposal of both electronic and paper clinical records.

C1.9(v) Where a Laboratory wishes to retain old health information (as defined by standard **S1.9**) for statistical reasons, the data should be de-identified, if possible.

C1.9(vi) All result data on individuals should have electronic audit trails to record:

(a) the original data with time and date of entry

(b) the name of the person authorising the result, with time and date of authorisation unless the result has been auto-validated

(c) the date and time of each report and to whom it was reported, each time a report is issued includes preliminary, amended and verbal reports

(d) details of any data modification after authorisation, together with the time, date and identity of the person who modified the data.

S1.10 The Laboratory must create and maintain a register of data that have been deleted or destroyed including:

(a) the individual to whom the data related

(b) the period of time that the data covered

(c) the date that the data were deleted or destroyed

(d) the person who authorised the data to be deleted or destroyed.

S1.11 The Laboratory must create and maintain a register of data that have been transferred to another individual or organisation including:

(a) the individual to whom the data relate

(b) the name of the organisation or individual to whom the data were transferred

(c) the person who authorised the transfer of data.

Openness and access

S1.12 In accordance with privacy legislation, the Laboratory must have a privacy policy that includes information on:

(a) management of health information

(b) the steps that an individual must take in order to obtain access to their health information.

C1.12(i) This policy document **must** be made available to anyone who asks for it.

C1.12(ii) The Laboratory's privacy policy should include:

(a) the privacy legislation that the Laboratory is bound by

(b) any exemptions that apply to the Laboratory under the relevant legislation

(c) a statement explaining that an individual can obtain more information, upon request, about the way the Laboratory manages personal information

(d) the reasons certain types of information are collected

(e) any routine procedures for collecting, holding and disclosing information, including services that are outsourced

(f) any laws that require the Laboratory to disclose information to other organisations (e.g. notifiable diseases)

(gi) information on how to handle requests for access to information

(h) the process for dealing with complaints about breaches of privacy

(i) the Laboratory's contact details.

C1.12(iii) Depending upon the size of the Laboratory or Laboratory network, it is recommended that the organisation appoint a designated privacy officer.

S1.13 On request by an individual, the Laboratory must take reasonable steps to let that individual know whether health information is held relating to them, and to let the individual know in general terms:

(a) the nature of the information

(b) how the Laboratory collects, holds, uses and discloses the information.

S1.14 If the Laboratory holds health information about an individual, it must provide the individual with access to their own health information upon request. In certain circumstances access may be denied. A Laboratory must provide reasons in writing to an individual for denying them access to their health information.

C1.14 Within the Laboratory's privacy policy, it is recommended that the Laboratory should have an escalation procedure to deal with requests for health information. In most circumstances, it would be preferable that individuals obtain their records through their requesting medical practitioner.

Access to health information may be denied to an individual if:

(a) providing access would pose a threat to the life or health of any person

(b) providing access would have an unreasonable impact on the privacy of other individuals

(c) the information relates to existing or anticipated legal proceedings between the Laboratory and the individual, and the information would not be accessible during those proceedings

(d) the information is otherwise subject to legal professional privilege

(e) providing access would reveal the intentions of the organisation in relation to negotiations (other than about the provision of a health service) with the individual, exposing the organisation unreasonably to disadvantage

(f) providing access would be unlawful

(g) denying access is required or authorised by or under law

(h) providing access would be likely to prejudice an investigation of possible unlawful activity

(i) providing access would be likely to prejudice a law enforcement function performed by, or on behalf of a law enforcement agency

(j) the request for access is of a kind that has been made unsuccessfully on at least one previous occasion and there are no reasonable grounds for making the request again; or

(k) the individual has been able to access his or her health information and is making unreasonable and repeated requests for the same information in the same form.

None of the circumstances listed above compel a Laboratory to refuse to provide an individual with access to his or her health information.

Use of identifiers and anonymity

S1.15 A Laboratory must only assign external identifiers to individuals if they are reasonably necessary for the Laboratory to function effectively.

C1.15 While most privacy legislation indicates that individual identifiers should only be assigned where deemed reasonably necessary, good Laboratory practice would indicate that most, if not all, Laboratories need to assign identifiers to individual patients in order to carry out their functions safely and effectively in the best interest of the patient.

S1.16 A Laboratory must not adopt an identifier of an individual that has been assigned by an agency of the Australian Government (e.g. a Medicare number or Australian Government Department of Veterans' Affairs number) as its own identifier of that individual, except where such use has been authorised.

C1.16 The Council of Australian Governments (COAG) has tasked the National eHealth Transition Authority with the development and implementation of a national infrastructure that enables unique health care identification of both consumers (Individual health Identifier — IHI) and providers (Healthcare Provider Identifier — HPI) within the health sector.

S1.17 Where it is lawful and practicable, individuals must have the option of not identifying themselves when entering into transactions with the Laboratory.

C1.17(ii) Without identifying information, it should be recognised that Specimens could not be tested in parallel, or reported in a cumulative form, which would impact on optimum patient care.

In some situations it may be unlawful to provide a service anonymously. For example, where an individual is diagnosed with a notifiable disease, some state and territory laws require providers to collect identifying information.

C1.17(ii) Without identifying information, patients will not be eligible for Medicare rebates in circumstances where they may otherwise be eligible.

C1.17(iii) A Laboratory may use an identifier assigned by another organisation (including state and territory public sector organisations) as its own identifier of an individual if:

(a) the individual has consented to the adoption of the identifier; or

(b) the adoption of the identifier is necessary for the Laboratory to fulfil its obligations to, or requirement of, the other organisation.

Inter-jurisdictional data flows

S1.18 An organisation in one jurisdiction must not transfer health information about an individual to someone in another jurisdiction (other than the organisation or the individual), except in the following circumstances:

(a) the organisation reasonably believes that the recipient of the information is subject to similar privacy principles

(b) the individual consents to the transfer

(c) the transfer is necessary for the performance of a contract between the individual and the organisation

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party

(e) the transfer is for the benefit of the individual, and it is impractical to obtain the individual's consent to that transfer, and if it were practicable to obtain such consent, the individual would be likely to give it

(f) the organisation has taken reasonable steps to ensure that the transferred information will not be used or disclosed inconsistently with National Privacy Principles

(g) the transfer is authorised by any other law; or

(h) the organisation reasonably believes that the transfer is necessary to lessen or prevent a serious or imminent threat to an individual's life, health, safety or welfare, or a serious threat to public health or safety.

Transfer or closure of the Laboratory

S1.19 Where a Laboratory is to be closed down, sold, amalgamated or otherwise transferred to another provider, appropriate steps must be taken to:

(a) make referring practitioners aware of the change

(b) inform referring practitioners about the proposed arrangements for the transfer or storage of records.

S1.20 Where an individual requests that their records be transferred to another provider, the closing Laboratory must provide the individual or the nominated alternative provider with the health record of the individual.

2. Documentation

(Refer to Standard 3, Standard 4 and Standard 6 in *Requirements for Medical Pathology Services*)

S2.1 The Laboratory must document security policies and procedures for the receipt of requests and transmission of reports, including electronic messaging.

C2.1 The documented security policy should include:

(a) the roles and responsibilities of Laboratory staff handling pathology orders and reports (including receipt and dispatch)

(b) details of the standards and specific requirements relating to the confidentiality, authenticity, integrity and availability of electronic pathology messages

(c) access rights and controls, including details about what these are and who they relate to, in relation to transmission of electronic pathology messages

(d) the processing of electronic request and electronic report message acknowledgments

(e) storage and archiving requirements, specifically in relation to the transmission of electronic pathology messages.

S2.2 The Laboratory must ensure designated staff are trained to support the transmission, handling, storage and archiving of pathology messages, including electronic messages.

S2.3 Any breach of security related to the electronic messaging of pathology data must be recorded. Procedures and systems must be reviewed and remedial action must be taken and subsequently monitored.

S2.4 The Laboratory must undertake internal audits of procedures to ensure these standards and guidelines are operating as required.

3. Security of storage

(Refer to Standard 1 and Standard 3 in *Requirements for Medical Pathology Services*)

S3.1 To ensure the secure storage of systems data, technological and procedural mechanisms must be established to ensure that:

(a) confidentiality is maintained

(b) information is accessible only to authorised users

(c) the integrity of information is maintained

(d) the accuracy and completeness of information and processing methods is maintained

(e) the availability of systems and services meets the needs of authorised users with regard to information and associated assets.

S3.2 Pathology systems contain sensitive, critical and valuable information, and system access controls must be in place to protect the information from being improperly disclosed, modified, deleted or rendered unavailable.

C3.2 The secure storage of data is required to reduce the threat of unauthorised access or usage or acts that may inadvertently or maliciously:

(a) risk the availability, authenticity, integrity and confidentiality of electronic records from the point of their creation to the point of their intended use

(b) allow unauthorised copying or replication of data or information

(c) disclose information to unauthorised personnel

(d) act as a gateway for unauthorised access by others

(e) infect systems with computer malware (e.g. viruses, trojans or worms).

There is a balance between applying security controls and allowing the ready exchange of information that is required by pathology Laboratories.

4. Security of data management (including access)

(Refer to Standard 1, Standard 3 and Standard 4 in *Requirements for Medical Pathology Services*)

S4.1 Data must be managed to protect its integrity.

S4.2 Each Laboratory or Laboratory network must identify at least one person whose role includes:

(a) identifying, documenting and maintaining information about databases within the system (e.g. patients, referring doctors and Laboratory staff)

(b) ensuring that the system is available when required

(c) ensuring that data are robust and reliable

(d) identifying data retention periods

(e) ensuring archived data are retrievable in a usable form

(f) ensuring formal plans exist for the retiring or destruction of data and/or systems

(g) assigning user identification and access levels all users including non-Laboratory personnel with access to the results database such as hospital ward or clinical staff.

S4.3 Each user, including non-Laboratory personnel, must have unique user logins and appropriate access levels.

5. Security of messaging

(Refer to Standard 1 and Standard 6 in *Requirements for Medical Pathology Services*)

S5.1 To ensure the secure and confidential messaging of electronic pathology reports, the Laboratory must:

(a) ensure the completeness, accuracy and integrity of electronic messages (i.e. certainty that the message has not been altered during transmission)

(b) ensure the pathology Laboratory message can be authenticated by the recipient.

C5.1(i) To ensure the secure and confidential messaging of electronic pathology requests and reports, Laboratories should:

(a) authenticate the originator of the pathology request

(b) acknowledge receipt of incoming messages

(c) authenticate the recipient of the pathology report.

C5.1(ii) Electronic request messages cannot be considered as successfully delivered until a transport acknowledgment message has been received, confirming delivery.

C5.1(iii) Electronic report messages cannot be considered as successfully delivered until a transport acknowledgment message has been received, confirming delivery. It is recognised that clinical software receiving report messages may not send an acknowledgment. However, software vendors should be encouraged to include this feature in their products.

C5.1(iv) Laboratory acknowledgment of an electronic request does not constitute a contract to undertake services; it indicates a willingness and capability to perform or refer the requested services when appropriate Specimens are received by the Laboratory.

C5.1(v) With faxed or SMS messaged reports, particular attention should be given to recipient authentication before transmission of the result.

C5.1(vi) Record of receipt of an electronic acknowledgment message forms part of the electronic patient record.

S5.2 Whenever a message is transmitted via a public network, it must be appropriately encrypted to protect the confidentiality of data and prevent unauthorised access during transmission.

C5.2(i) Data can be encrypted using accepted transport security protocols such as secure socket layer (SSL) or public key encryption mechanisms such as public key infrastructure (PKI) (e.g. HeSA or Pretty Good Privacy®). Public key encryption ensures strong authentication of sender and recipient.

C5.2(ii) Encryption should be considered in private networks as part of information security risk management.

C5.2(iii) Procedures should be in place to deal with the following circumstances:

(a) A result message returns a 'failure' acknowledgment message. For example, where there is a failure to deliver a report.

(b) No acknowledgment message is received within a specified period. The period of time to wait for an acknowledgment message may be agreed between the Laboratory and receiver but in general should be no longer than one working day for routine reports. Failure to receive an acknowledgment message indicating a successful receipt should initiate a Laboratory alert and possibly lead to delivery of results by another method.

(c) Urgent reports:
Receipt of a 'failure' acknowledgment message or failure to receive any acknowledgment within an appropriate timeframe for messages containing urgent results should initiate immediate action to deliver reports through an alternative channel, such as phone or fax. In general, failure to receive a successful acknowledgment within one hour of message transmission should prompt review action by the Laboratory.

(d) Clinically significant reports:
These reports should be treated with a protocol similar to urgent reports (see G5.2(c)). Examples of clinically significant reports include, but are not limited to, critical abnormalities or marked and unexpected changes from previous results.

(e) The appropriate procedures to deal with these cases should also be documented and a log maintained of such exceptions and the subsequent actions taken to ensure result delivery.

6. Compliance with electronic messaging standards

(Refer to Standard 2, Standard 3 and Standard 6 in *Requirements for Medical Pathology Services*)

Electronic communication of requests and reports should comply with protocols set out in the Standards Australia publications AS4700.2–2004 *Implementation of Health Level Seven (HL7)* and HB262–2002 *Guidelines for pathology messaging between pathology providers and health service providers* and their subsequent revisions.

Where an electronic request is not accompanied by a paper request form, processing of the electronic request should comply with current Medicare Australia regulations for processing such requests, in order to be eligible for reimbursement under the Medicare Benefits Schedule.

The Laboratory should have their electronic messages certified for compliance against AS4700.2–2004 *Implementation of Health Level Seven (HL7)* by an accredited message compliance organisation such as the Australian Healthcare Messaging Laboratory (AHML), which has recently been accredited by the National Association of Testing Authorities (NATA).

7. Business continuity planning (including archiving)

(Refer to Standard 2 and Standard 3 in *Requirements for Medical Pathology Services*)

S7.1 The Laboratory must have a business continuity plan.

C7.1(i) The business continuity plan should include procedures for regular backup of electronic data, systems recovery, application recovery, and data recovery or restoration. It should also include procedures for assessing the extent of damage or data loss in the event of a disaster.

C7.1(ii) The business continuity plan should include alternative procedures to enable continued operation, receipt of requests, and delivery of reports.

C7.1(iii) Standards for a business continuity plan are described in AS/NZS ISO/IEC 17799:2001 *Information Technology — Code of Practice for Information Security Management*.

C7.1(iv) All data should be retained in either an archival or online format for appropriate periods to comply with legal requirements. This will vary according to the test(s) performed (histology or cytopathology versus blood tests), the patient's age and jurisdiction-specific legislation and regulations.

C7.1(v) In general, data should be retained for as long as technically feasible in an online, directly accessible format to permit comparison of current results with historical results. If the archived data are not immediately available, the procedure to find and restore data to the active database should be documented.

8. Laboratory audit trail

(Refer to Standard 4 and Standard 6 in *Requirements for Medical Pathology Services*)

S8.1 Laboratory staff who have access to electronic pathology data and the ability to trigger transmission, change or correction of electronic data must have individual security logins.

S8.2 If a paper request is received, then a scanned, hard copy or the original request must be stored keeping all the original content, date, time, location and originator of the request. The same information provided in electronic requests must also be stored. Any changes to the request must be stored with the original.

C8.2 The Laboratory will also need to be cognisant of additional requirements set out by Medicare Australia.

S8.3 Receipt of a request initiates the audit trail. If acknowledgment is received from any transmission (including interim reports) this must also be recorded. The audit trail must include:

(a) request registration

(b) patient record linking and merging

(c) patient master index transmission (e.g. name of the hospital)

(d) validation or auto-validation

(e) results entry and comments

(f) results amendments

(g) results transmission (e.g. date, time and mode)

(h) patient result access by non-Laboratory staff (see also S4.2(g)). Alternatively, where it is deemed impractical to include access by such staff into the audit trail then such staff must have received adequate training in the area of jurisdictional privacy legislation

(i) an audit trail of any subsequent changes to a previously validated report.

C8.3(i) Mode of transmission includes printing, faxing, email and electronic transmission. It also includes verbal reporting by phone.

C8.3(ii) The audit trail is considered part of the patient record.

C8.3(iii) Current paper-based and intra-Laboratory systems provide for traceability of requests, technical procedures, results and reports. These capabilities need to be maintained and enhanced in electronic systems, so that access, actions and changes can be traced where and when necessary.

C8.3(iv) Read-only access of patient-identified data by Laboratory staff should be included as part of the audit trail.

S8.4 The pathology Laboratory collecting the audit trail information should notify its staff (and anyone else who accesses patient records):

(a) that their access to patient records will be recorded on the audit trail

(b) for what purposes the audit trail information will be used

(c) to whom the audit trail information may be disclosed.

Appendix A Online versions of national, state and territory privacy legislation (Informative)

National

Privacy Act 1988
http://www.privacy.gov.au/publications/privacy88_030706.pdf

National Privacy Principles
http://www.privacy.gov.au/publications/npps01.pdf

Privacy (Private Sector) Amendment Regulations 2006 (No. 1) Statutory Rules No. 301
http://www.privacy.gov.au/publications/2006no1reg.pdf

Australian Capital Territory

Health Records (Privacy and Access) Act 1977
http://www.legislation.act.gov.au/a/1997-125/current/pdf/1997-125.pdf

New South Wales

Privacy and Personal Information Protection Act 1998
http://www.austlii.edu.au/au/legis/nsw/consol_act/papipa1998464

Health Records and Information Privacy Act 2002
http://www.austlii.edu.au/au/legis/nsw/consol_act/hraipa2002370

Northern Territory

Information Act 2002
http://www.nt.gov.au/nreta/foi/infoact.html

Queensland

Information Standards 42A (Health)
http://www.governmentict.qld.gov.au/02_infostand/standards/is42a.pdf

South Australia

Information Privacy Principles 1989
http://www.premcab.sa.gov.au/dpc/publications_circulars.html

Tasmania

Personal Information Protection Act 2004

http://www.egovernment.tas.gov.au/themes/information_security__and__management/personal_information_protection

Victoria

Information Privacy Act 2000
http://www.dms.dpc.vic.gov.au/Domino/Web_Notes/LDMS/PubLawToday.nsf/0/b1a1dfc4eebe1eeaca256e5b00037a1d/$FILE/00-98a001.pdf

Health Records Act 2001
http://www.health.vic.gov.au/healthrecords

Western Australia

Health Act 1911
http://www.newpublichealthact.health.wa.gov.au/home

Please note: at the time of publication there was no state-specific privacy legislation in Western Australia.

Bibliography

1. AS4700.2–2004 Implementation of Health Level Seven (HL7)

2. AS5017 Health Care Client Identification

3. AS ISO 17799 Information Security Management

4. AS/NZS ISO/IEC 17799:2001 Information Technology – Code of Practice for Information Security Management

5. HB 174 Information Security Management Implementation Guide for the Health Sector

6. HB262–2002 Guidelines for pathology messaging between pathology providers and health service providers

7. Privacy Policy in Community Pathology (AAPP), revision 1.2 2002. <http://www.aapp.asn.au/privacy.html>

Further information

Other NPAAC documents are available from:

NPAAC Secretariat
Primary Care, Diagnostics & Radiation
Oncology Branch
Department of Health
GPO Box 9848 (MDP 951)
CANBERRA ACT 2601

Phone: (02) 6289 4017
Fax: (02) 6289 4028
Email: npaac@health.gov.au
Website: www.health.gov.au/npaac