



**Pathology Result Reporting Package
(v1.0 Draft)**

Business Architecture v2.0

1 September 2008

Draft for comment - Commercial-in-confidence

National E-Health Transition Authority Ltd

Level 25

56 Pitt Street

Sydney, NSW, 2000

Australia.

www.nehta.gov.au**Disclaimer**

NEHTA makes the information and other material ('Information') in this document available in good faith but without any representation or warranty as to its accuracy or completeness. NEHTA cannot accept any responsibility for the consequences of any use of the Information. As the Information is of a general nature only, it is up to any person using or relying on the Information to ensure that it is accurate, complete and suitable for the circumstances of its use.

Document Control

This document is maintained in electronic form. The current revision of this document is located on the NEHTA Web site and is uncontrolled in printed form. It is the responsibility of the user to verify that this copy is of the latest revision.

Security

The content of this document is confidential. The information contained herein must only be used for the purpose for which it is supplied and must not be disclosed other than explicitly agreed in writing with NEHTA.

Copyright © 2008, NEHTA.

This document contains information which is protected by copyright. All Rights Reserved. No part of this work may be reproduced or used in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems—without the permission of NEHTA. All copies of this document must include the copyright and other information contained on this page.

Document Information

Change History

Version	Date	Author	Comments
3.0	1/09/2008	NEHTA	Package v1.0 Draft update
1.3	28/08/2008	NEHTA	Package v1.0 Draft update
1.2	20/08/2008	NEHTA	Draft subtitles amended, page break modifications
1.1	15/5/2008	Siobhan Jenks	Draft re-imported into template to remove formatting corruption
1.0	9/04/2008	NEHTA	Draft released for comment

Authorisation History

Version	Date	Status	Comments
3.0	1/09/2008	Draft for Review	New formatting added
1.3	28/08/2008	Draft for Review	New formatting added
1.2	20/08/2008	Draft for Review	New formatting added
1.1		Draft for Review	New formatting added
1.0	9 Apr 2008	Draft Approved	Draft approved for initial review release

Distribution List

Name	Role	Comments
	Subject Matter Reviewer	To verify that the factual content is correct
	Format Reviewer	To verify that the document or suite of documents has consistency and uses approved format
	Specialist Reviewer	To verify some specialist knowledge. For example, a Word formatting expert to check a template before release.
	Approver	The owner of the document approves after the review process is finalised.
	General Readership	For information

Table of Contents

Document Information	iii
Change History	iii
Authorisation History	iii
Distribution List.....	iii
Table of Contents	iv
Preface	vii
Document Purpose	vii
Intended Audience.....	vii
Document Map.....	vii
NEHTA Interoperability Framework	viii
Organisational.....	viii
Informational	viii
Technical.....	ix
Definitions, Acronyms and Abbreviations.....	ix
References and Related Documents	ix
1 Overview	10
1.1 Background and Purpose	10
1.2 Business Context	10
1.3 Business Profile	11
1.4 Scope	11
1.4.1 Inclusions	11
1.4.2 Exclusions.....	11
1.5 Assumptions and Dependencies	12
1.6 Process Modelling Approach	12
2 Pathology Reporting Community	13
2.1 Overview.....	13
2.1.1 Actor Roles	14
2.1.2 Information Entities.....	16
2.1.3 Interactions between Community Roles.....	18
2.2 Community Policies.....	20
2.2.1 AS 4633-2004	20
2.2.2 Chain of Information Custody	21
2.2.3 Requirements for Information Communication.....	23
2.2.4 Patient Identification	23
2.2.5 Provider Identification.....	24
2.2.6 Information Privacy.....	24
3 Business Processes	29
3.1 Exchange Report	29
4 Business Requirements	33
4.1 Functional	34
4.1.1 1.0 Compile Report	34
4.1.2 2.0 Determine Receiver	38
4.1.3 3.0 Distribute Report	41
4.1.4 4.0 Encrypt Message	48
4.1.5 5.0 Sourcing Report	52
4.1.6 6.0 Acknowledgement Management.....	57
4.1.7 7.0 Report Monitoring	59
4.1.8 8.0 Manage Report Storage	62
Definitions	67

Shortened Terms	67
Glossary	68
References	70
Package Documents	70
References	70
Related Reading	72

This page is intentionally left blank.

Preface

Document Purpose

This document has been structured to present the Business Architecture of the Pathology Domain in a manner compliant with the [NEHTA Interoperability Framework \(IF\)](#), and capturing the business requirements for the Pathology Result Report Exchange. As such, it documents the 'AS IS' and the 'TO BE' Business Architecture relationships.

Intended Audience

This document is intended to be read by jurisdictional ICT managers, clinicians involved in Clinical Information System specifications, software architects and developers, and implementers of Clinical Information Systems in various health care settings.

It is reasonably technical in nature and expects the audience to be familiar with the language of health data specifications, and to have some familiarity with health information standards and specifications, including the NEHTA IF.

Document Map

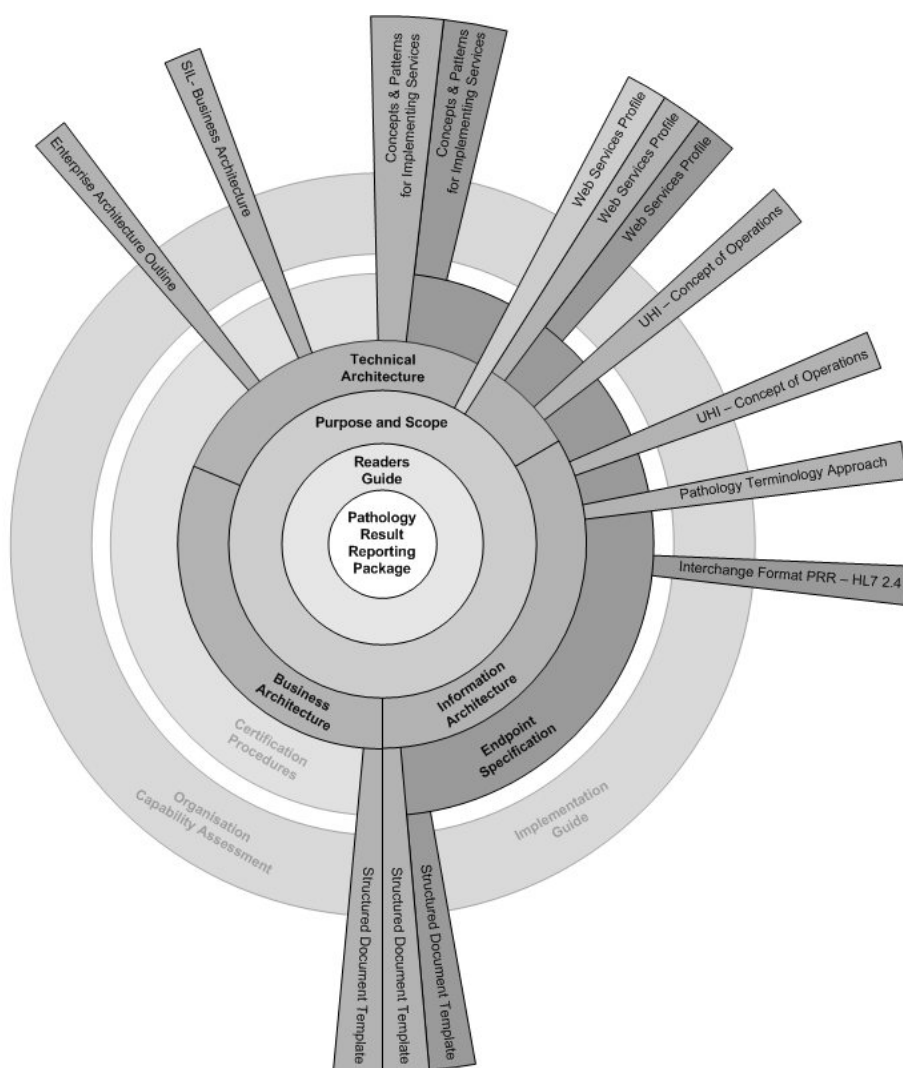


Figure 1: Document Map

The diagram in Figure 1 shows where the Business Architecture document fits into the entire Pathology Result Reporting Package. It is central to an understanding of the whole package. As rings ripple outward, the documents become more and more detailed.

The Package Document Map is designed to show the hierarchy of core documents within the package, and their relationships to ancillary documents. Core package documents are represented as arcs, while ancillary documents (or references to such) appear as radiating spokes. Note that, due to the 'many-to-many' relationships within the package, some ancillary documents appear more than once, and have typically been grouped for clarity.

It is recommended that readers commence with documents at the centre of the map (i.e. the 'Readers' Guide', and 'Purpose and Scope'), working outwards to the detailed, technical documents as needed. It is recommended that business sponsors focus upon core documentation, while technical implementers also include ancillary document reading.

Core documents are explained in the Readers' Guide [PATH-PRR-RG].

NEHTA Interoperability Framework

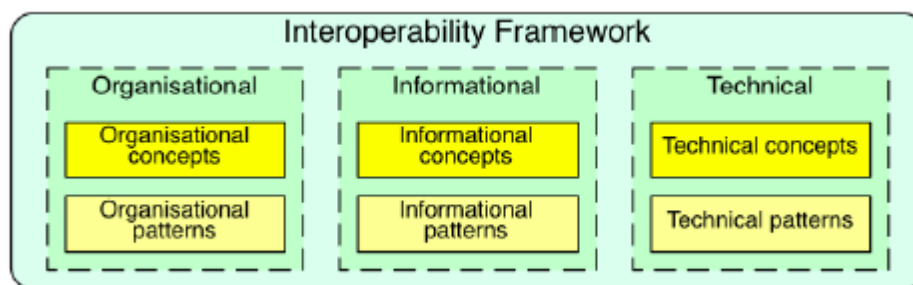


Figure 2: NEHTA Interoperability Framework

The IF [[INTER2007](#)] provides definitions for each interoperability perspective.

Organisational

The Organisational Interoperability Framework (OIF) addresses business contexts, legal and policy issues relevant to the understanding, specification and deployment of e-health systems.

The OIF allows for the description of business processes, business policies and organisational structures, covering the scope of intra-organisational, inter-organisational and cross-jurisdictional interactions.

This perspective makes use of the following OIF concepts:

- Community objectives
- Business policies (external to, or defined by, the community)
- Community roles
- Business processes
- Business services.

Informational

The Informational Interoperability Framework (IIF) addresses the semantics of information relevant to the comprehension, specification and deployment of e-health systems. The IIF allows for the description of key information components and their relationships.

Technical

The Technical Interoperability Framework (TIF) provides a framework for specifying functionality to be delivered by the technologies employed within e-health applications, oriented to business purpose, as documented by the organisational concepts and patterns. This framework recommends the use of a Service-Oriented Architecture (SOA).

Definitions, Acronyms and Abbreviations

For a lists of abbreviations, acronyms and abbreviations, see the [Definitions section](#) at the end of the document, on page 67.

References and Related Documents

For a list of all referenced documents, see the [References](#) at the end of the document, on page 70.

1 Overview

1.1 Background and Purpose

This document has been produced as part of the NEHTA Pathology Program's Pathology Result Reporting Package. It defines the Business Architecture. Information contained within this document was sourced from the Pathology Communications project conducted by AAPP and NEHTA in 2006 and has been refined for the purposes of the Pathology Result Reporting Package.

The purpose of this document is to specify the Business Architecture for Pathology Reporting in Australia. Consequently, this document should be used to consolidate the requirements for solutions which engage in the process of sending or receiving pathology result reports.

The document focuses on requirements and functions, without detailing quantifiers such as time, sizes, quantities, and business rules. It is assumed that the document will prompt discussion on the scope and boundaries of each individual information transaction.

1.2 Business Context

This package is designed to deliver Pathology Result Report services, supported by appropriate business processes, people and technology.

The primary objective of the package is to identify the appropriate information model(s) and data exchange capability for the differing environments in the Pathology Community, leading to appropriate national End Specifications

The key performance indicators for the successful completion of the package are the implementation and approval of the information models and data exchange capability solutions within the Pathology Community, thereby extending the national e-health solution.

The business outcomes of package implementation within the Pathology Community will be achieved by reviewing the:

- Current Business Processes
- Ability of the Pathology Community to support the proposed e-health solution
- Ability of pathology report-related personnel to support changing business processes
- Technical and funding requirements for the recommended options
- Ability to establish the appropriate relationships within the Pathology Community to support the strategic direction of the package.

Business processes are currently not standardised between different Pathology Community participants, although they may share the same patients and information types. Standardisation of the business processes that have a direct relationship with the proposed solution (e.g. information sharing) can enhance continuity of care across primary and secondary care providers and positively affect clinical practise outcomes.

Primary objectives of the package include the sharing of information resources; improving access to health care data and information while protecting individual's privacy; and allowing health professionals to work together more efficiently to provide quality health care to their communities.

1.3 Business Profile

Transactions are primarily clinical, based upon end-users collecting highly sensitive patient information mainly within a clinical setting. This information is essential for decision making at point of care, and for immediate and future care planning.

Additional data collection will occur at the Pathology Report Recipient practice and/or the Pathology Provider location, and needs to be reconciled within the Pathology Provider Laboratory Information System. This model is mainly centralised per Pathology Provider but some additional information may be collected outside the Pathology Provider environment. The user base currently consists of clinical staff, but may be extended to the subject of care in the future.

In the event of system downtime, the existing paper-based Pathology Result Reporting could serve as a substitute method for recording test results. Information required at distant locations could be faxed or emailed, as is currently done, with the additional risk of unauthorised recipients also obtaining the data. Under these conditions the quality and distribution of the information is likely to be lower than would otherwise be the case, and could negatively affect patient care if there were extended periods of downtime, especially during emergency situations.

1.4 Scope

This section highlights the scope of the requirements addressed in this document. The package scope is defined in detail in the Purpose and Scope document [PATH-PRR-PS].

1.4.1 Inclusions

This document deals with the following requirements:

- The creation of an electronic version of the Pathology Result Report allowing for flexibility, versioning and change across multiple implementation solutions
- The ability to determine the delivery location (service end-point) for the Pathology Report Recipient, and subsequent notification
- Allowing for multiple methods of delivery (electronic, manual or both) to cater for different connectivity implementations (i.e permanently or periodically connected report recipients)
- Ensure that the information delivered is secure, precise, and has not been subject to tampering
- Enable Pathology Result Report life cycle tracking, by providing acknowledgments from the recipient on the phases of the report sourcing and distribution.

1.4.2 Exclusions

This document does not deal with the requirements for:

- Pathology Result Report Service Requests (i.e. only the results of the Pathology Report request are covered)
- National E-Health Infrastructure aspects that are not specific to Pathology Result Reporting (i.e. it is understood that these services have their own requirement gathering processes and, consequently, this document will refer to requirements upon those services without specifying them in depth).

1.5 Assumptions and Dependencies

The table below lists assumptions made within this document, and dependencies upon other documents. Please refer to the Glossary on Page 67.

Item	Description
1	<i>Pathology Providers</i> can exchange reports without using an Intermediary.
2	The use of an <i>Intermediary</i> is dictated by the Vendor Software and is therefore not only dependent on connectivity but also upon the consolidation of the Pathology Provider results.
3	Currently, the majority of the <i>Pathology Report Recipients</i> use Intermediaries.
4	Existing business processes are designed to comply with policy requirements, particularly those relating to the 'Chain of Information Custody.'
5	<i>SIL</i> will contain references to the service endpoints, and capabilities for the Pathology Community, and will be used to identify the <i>Pathology Report Recipients</i> and <i>Intermediaries</i> .
6	Manual notification of the <i>Pathology Report Recipient</i> is a business process that is currently in place.
7	An authorised <i>Intermediary</i> can act on behalf of the Pathology Report Recipient.
8	Notifications and Acknowledgements do not contain any personal or health information about a patient and do not require encryption.
9	Authorisation, Authentication and Encryption of use case descriptions are addressed by NASH documentation.
10	<i>SIL</i> use case descriptions are documented in the <i>SIL</i> specifications.

1.6 Process Modelling Approach

The processes and associated business descriptions were modelled via background research and a series of interviews conducted in 2007 with a subset of subject matter experts initially involved to compile this document.

A model of the high level business process will differentiate between different participants: namely, the Pathology Provider, the Intermediary and the Pathology Report Recipient. The diagrams included in this document follow the Business Process Modelling approach and use the UML v2.0 notation for the graphical representations in this document. All models are documented in Sparx Enterprise Architect and a full model will be published via this document as HTML.

2 Pathology Reporting Community

2.1 Overview

NEHTA's Interoperability Framework (IF) defines a community as a collection of entities (e.g. individuals, organisations, information systems, resources, or various combination of these), established to meet a given objective.

The Business Architecture in this document is restricted to the Pathology Reporting Community and will be described from the Organisational interoperability perspective of the IF.

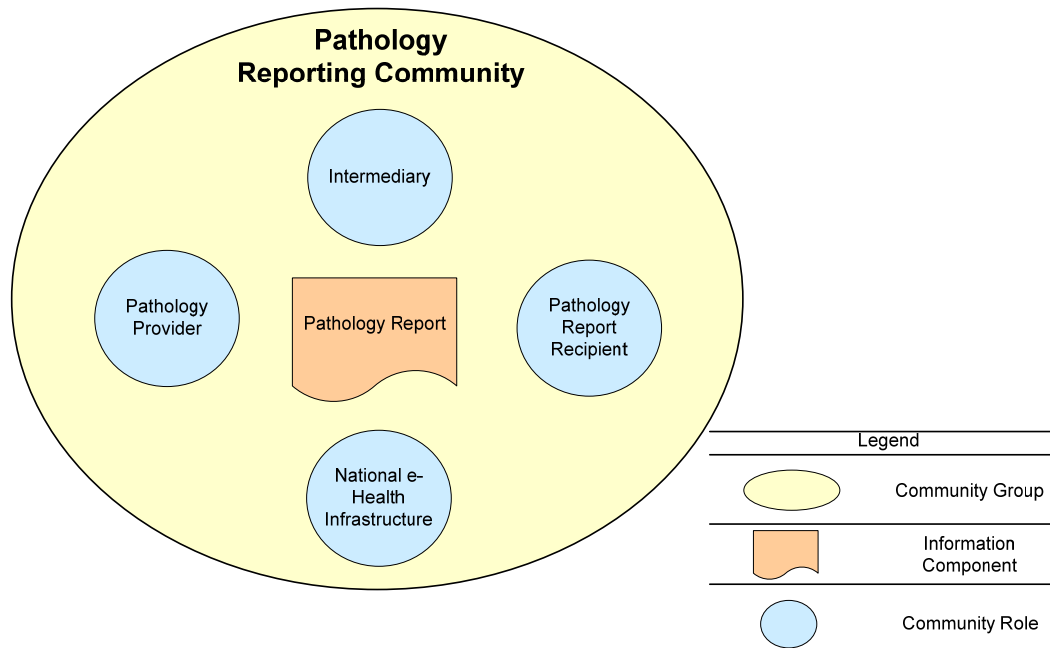


Figure 3: Pathology Report Recipient Community

The Pathology Reporting Community is the collection of entities (e.g. individuals, organisations, information systems, resources etc) established to manage the process of transferring Pathology Reports between a Pathology Provider and the intended Pathology Report Recipient(s).

As shown in Figure 3 the Pathology Reporting Community is defined in terms of four main community roles:

- **The Pathology Provider** is the entity that performs the pathology services
- **The Pathology Report Recipient** is the entity intended to receive a Pathology Report and may be an individual person, group, system or place
- **The Intermediary** is an entity that exists between the Pathology Provider and the Pathology Report Recipient to assist in the communication process
 - Intermediaries can serve both as a storage facility for disconnected parties, and a method for the aggregation of Pathology Reports from multiple Pathology Result Report Providers
- **The National E-Health Infrastructure** is a set of future services that will enable a common processing approach across the Australian e-health community, comprising authentication, identification and service location. It is proposed that the infrastructure will include:

- **The Unique Healthcare Identification Service**, which will enable the unique identification of both individuals (healthcare consumers) and Healthcare Providers (individual providers and organisations)
- **The National Authentication Service for Health (NASH)**, which will provide strong authentication credentials to individuals and organisations in the Health Community
- **The Service Instance Locator (SIL)**, which will be used by applications to locate the correct service endpoint when attempting to establish communications with a service.

Please note that these infrastructure components will not be available during the initial implementation of the Pathology Result Reporting Package.

2.1.1 Actor Roles

2.1.1.1 Pathology Provider

Description The *Pathology Provider* performs pathology services. The *Pathology Provider* in this context does not usually refer explicitly to a specialist medical practitioner in pathology but to an organisation and its associated infrastructure that support and provide pathology services.

Policy

- The *Pathology Provider* is responsible for preparing and providing a comprehensive and clinically meaningful report of the outcomes of a pathology request to a Pathology Report Recipient.

Example(s)

- Laboratory, Reference Laboratory

Actor Type Organisation, Primary

2.1.1.2 Pathology Report Recipient

Description A *Pathology Report Recipient* receives a Pathology Result Report. A Pathology Report Recipient can be an individual person, group, system or place

Policy

- The *Pathology Report Recipient* (or their employing organisation/agent) should have access to a management system to ensure that overdue or missing pathology reports are obtained, viewed and acted upon with a minimum of delay.

Example(s)

- Medical Practitioners including General Practitioners and Specialists
- Health Care Organisations including Hospitals, Community Centres and Aged Care Facilities
- Nurse Practitioners
- Patients
- Allied Health
- Medical records departments
- Public Health Registries
- Other Pathology Provider(s)
- Infection Control Committees, Tissue Audit committees, etc

Actor Type Organisation, Primary

2.1.1.3 Intermediary

Description An *Intermediary* acts as a storage facility for disconnected parties and provides a method of aggregation of *Pathology Reports* from multiple *Pathology Result Report Providers*.

Intermediaries are not considered to be trusted to view the contents of the *Pathology Result Report* that is sent from the *Pathology Provider* to the *Pathology Report Recipient*.

- Policy**
- An *Intermediary* is an entity that sits between two communicating parties.
 - The *Intermediary* has its own identity and is known to both parties that are communicating.
 - The *Pathology Result Report Provider* will be aware that they are dealing with an intermediary instead of directly with the *Pathology Report Recipient*.

- Example(s)**
- Supplier of a Notification Service
 - Supplier of a Sealed Report Store Service

Actor Type Organisation, Primary

2.1.1.4 National E-Health Infrastructure

Description Provides a set of services that will enable a common approach across the Australian e-health community regarding processes such as authentication, identification and service location.

- Policy**
- Enable the unique identification of both individuals (healthcare consumers) and Healthcare Providers (individual providers and organisations).
 - Provide strong authentication credentials to individuals and organisations in the Health Community.
 - Locate the correct service endpoint, when attempting to establish communications with a service.

- Example(s)**
- NASH, UHI, SIL

Actor Type Service, Primary

2.1.2 Information Entities

2.1.2.1 Pathology Report

Description	<p>A Pathology Result Report is defined (in Australian Standard: AS4700.2 - 2004 – Amendment 1, page 7) as</p> <p><i>"a set of one or more results and any associated interpretation usually generated in response to a request for Pathology. A report may include results previously reported and in some instances results from another request."</i></p> <p>The essence of a <i>Pathology Result Report</i> is the facilitation of the transfer of Pathology information, in whole or in part, from one healthcare provider or organisation to another.</p> <p>The <i>Pathology Result Report</i> can take several forms, including a:</p> <ul style="list-style-type: none"> • Report from a laboratory to the requesting clinician, whether they are in general practice or a hospital setting • Report from a reference laboratory to a requesting laboratory (the report may also be sent to the original requesting clinician) • Report from a laboratory to a shared electronic record • Report from a laboratory to a notification system or registry for notifiable or infectious diseases. <p>The common factor is that it is a communication of the results for a Pathology investigation(s) relating to a subject of care.</p>
Policy	<ul style="list-style-type: none"> • The issued report should meet the NPAAC and NATA requirements, and include sufficient information for the <i>Pathology Report Recipient</i> to optimise its value for patient care. The report should identify the original <i>Pathology Report Recipient</i> and other practitioners who have been sent a copy of the report
Example(s)	<ul style="list-style-type: none"> • Pathology Report

2.1.2.2 Acknowledgement and Notifications

Description	<p>Contains the status of a report or location, between the <i>Pathology Provider</i>, <i>Intermediary</i> and <i>Pathology Provider Recipient</i>.</p>
Policy	<ul style="list-style-type: none"> • For electronic delivery of reports, the <i>Pathology Provider</i> and <i>Pathology Report Recipient</i> should have mechanisms in place to record acknowledgments and notifications by the <i>Pathology Report Recipient</i> or <i>Pathology Provider</i>.
Example(s)	<ul style="list-style-type: none"> • Process Report Acknowledgment • Report Receipt Acknowledgment • Notifications

2.1.2.3 Supporting Terminology

Description	<p>Are the consolidated agreed terms that will be used by the Pathology Report, Acknowledgements and Notifications messages.</p>
Policy	<ul style="list-style-type: none"> • Population of the medical terms and references must comply with the existing standards.
Example(s)	<ul style="list-style-type: none"> • Systemised Nomenclature of Medicine Clinical Terms - Australian Extension (SCT-AU) • Logical Observation Identifier Names and Codes (LOINC)

2.1.2.4 Healthcare Identifiers

Description	Within the healthcare service delivery community, the process of positively identifying healthcare consumers involves matching data supplied by those individuals against data the healthcare provider holds about them. This entity contains the required data. [PATH-PRR-IA]
Policy	<ul style="list-style-type: none"> • Ensuring that reasonable steps are taken to protect the personal information and that only the appropriate health carer receives the data.
Example(s)	<ul style="list-style-type: none"> • Individual Healthcare Identifiers (IHIs) to identify all Australian healthcare consumers • Healthcare Provider Identifiers - Individual (HPI-Is) to identify individual healthcare providers (HPI-Is) such as general practitioners, clinicians, nurses and pharmacists • Healthcare Provider Identifiers – Organisation (HPI-Os) to identify healthcare organisations such as hospitals and clinics (HPI-Os).

2.1.2.5 NASH Credentials

Description	The strong authentication of healthcare providers is an important foundation service in the e-health community. For this reason, NEHTA plans to build and operate a new national service, called the National Authentication Service for Health (NASH). The entity NASH Credentials contains the required data [PATH-PRR-IA].
Policy	<ul style="list-style-type: none"> • Establish a single authoritative source providing strong authentication credentials for use in the Australian health sector. • Create a number of credential issuers across the sector, each able to create and issue local credentials using the central source. • Establish and operate an authentication service adoption program, intended to support both health software vendors and health jurisdictions in their own programs to incorporate strong authentication credentials into their applications and environments. Create a service to assist end users with the adoption and deployment of authentication tokens.
Example(s)	

2.1.2.6 Service Instance Locator (SIL)

Description	Applications that attempt to establish communications with a service will use a SIL to locate the correct service endpoint. [PATH-PRR-IA]
Policy	<ul style="list-style-type: none"> • Service endpoints for all message receivers must be stored in a SIL. • The SIL for a message receiver can be found using its HPI-O record.
Example(s)	<ul style="list-style-type: none"> • Store a set of Service Instance Records (SIRs). • Retrieve a set of Service Instance Records (SIRs).

2.1.3 Interactions between Community Roles

This section provides a high-level description of proposed community behaviour, by identifying a list of interactions between existing - and proposed - roles in the community. The existing roles are the *Pathology Provider*, *Intermediary* and *Pathology Report Recipient Organisation*. Two new roles, *SIL* and *NASH*, are introduced at this level.

These interactions can be used for subsequent detailed business process descriptions.

Two types of scenarios can be identified being:

- Permanently connected participants, typically comprising larger Pathology Report Recipients and Pathology Providers
- Periodically connected participants, typically comprising Pathology Report Recipients without permanent network access or with desktop software that is only configured for intermediary access.

2.1.3.1 Permanently Connected

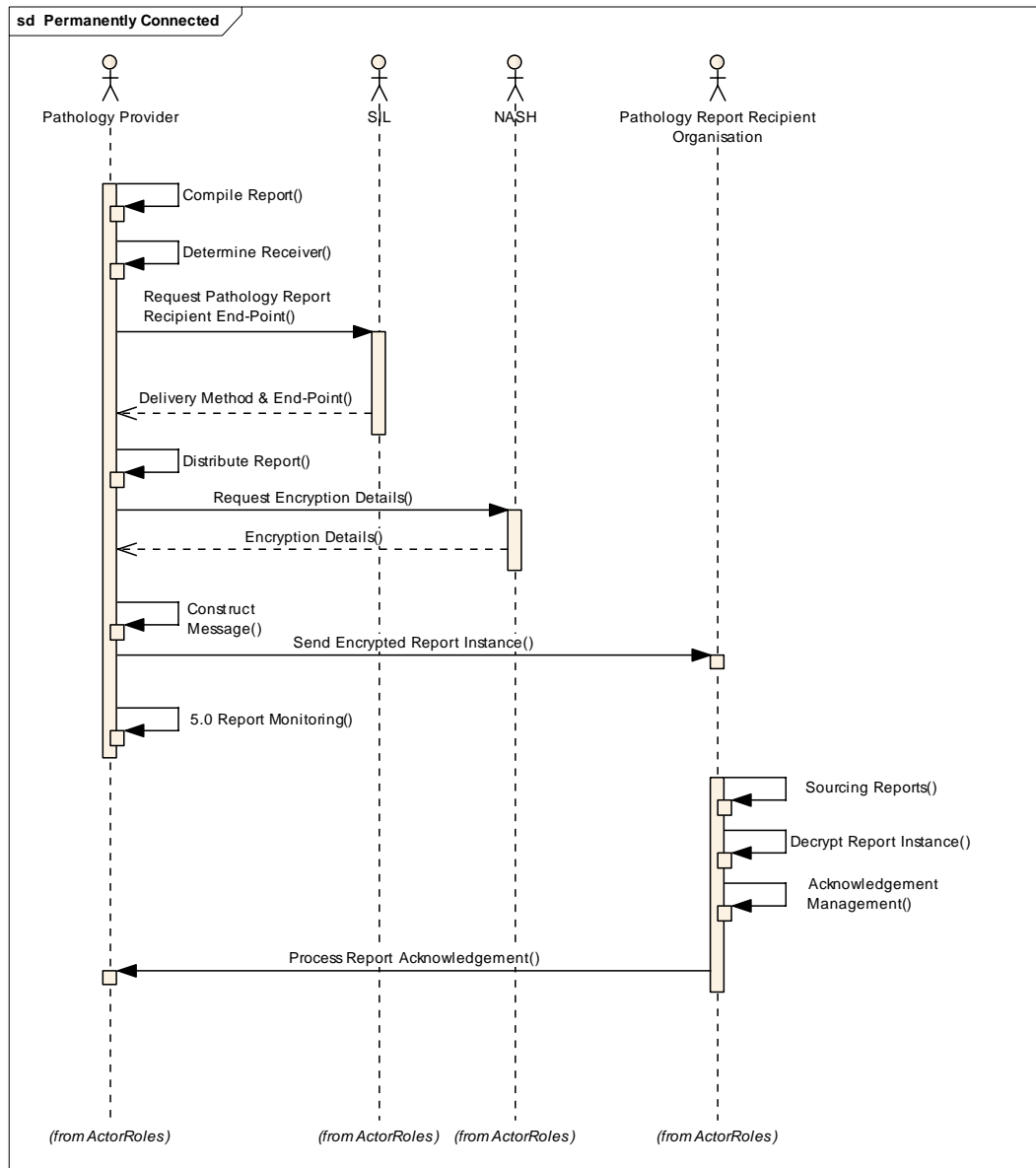


Figure 4: Permanently Connected Report Recipient Example

Note: This diagram is for example purposes only.

Figure 4 illustrates an example of permanently connected report recipients. The following interactions can be identified in this scenario:

1. The *Pathology Provider* requests the *Pathology Report Recipient Organisation* endpoint to establish the destination for the report.
2. The *SIL* responds with the endpoint and the preferred method of delivery which will be sent directly (direct put) to the *Pathology Report Recipient Organisation*, in this instance.
3. The *Pathology Provider* requests for the encryption details from the *NASH* to allow for encryption of the message with an approved certificate.
4. The *NASH* responds with the encryption details for the message.
5. The *Pathology Provider* distributes the encrypted Report Instance to the *Pathology Report Recipient Organisation*.
6. The *Pathology Report Recipient Organisation* sends a notification to the *Pathology Result Report Provider* to acknowledge the report has been successfully processed. This means that the report has been decrypted and its contents parsed.

2.1.3.2 Periodically Connected

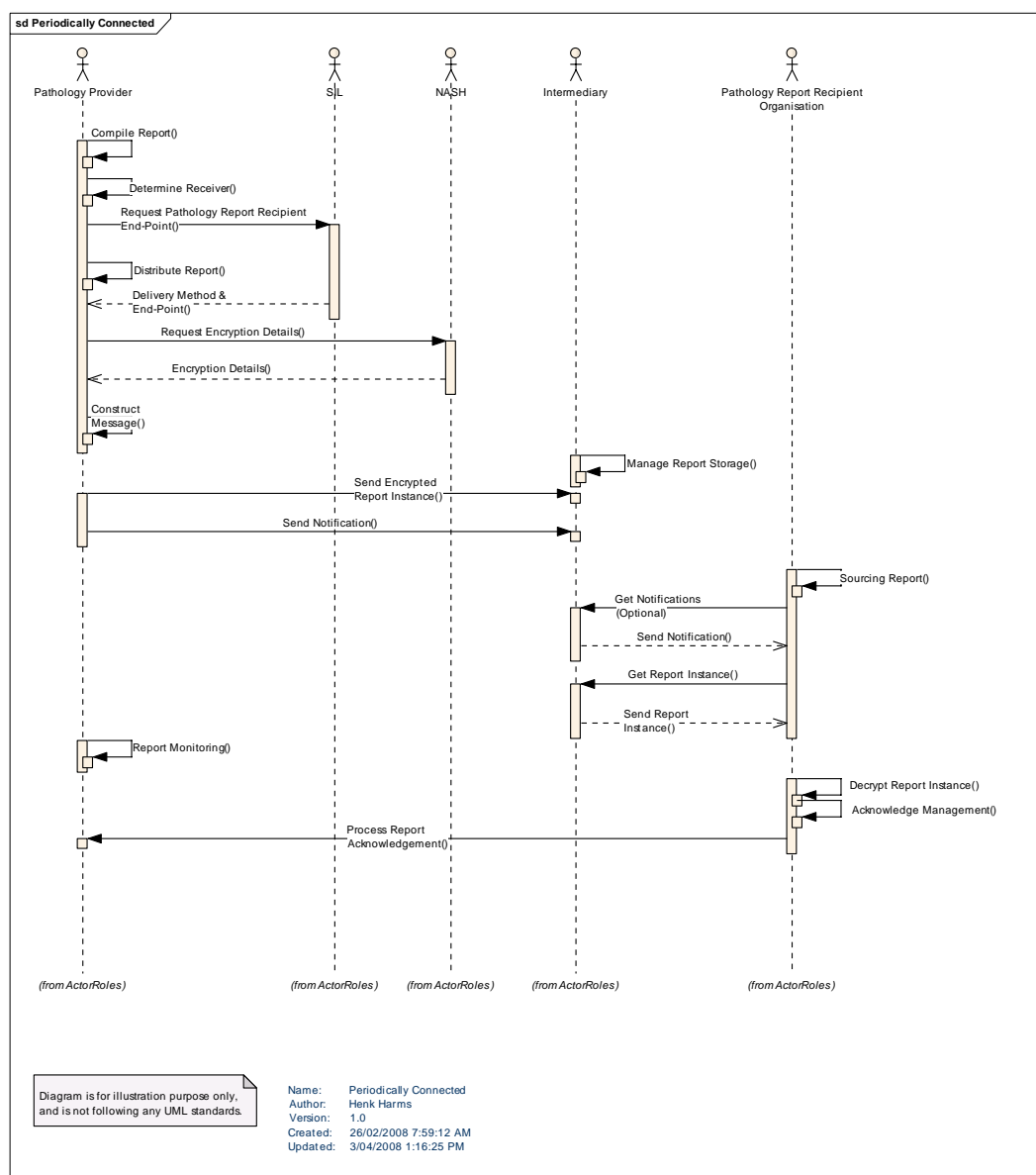


Figure 5: Periodically Connected Report Recipient Example

Note: This diagram is for example purposes only.

The following interactions can be identified in this scenario:

1. The *Pathology Provider* requests the *Pathology Report Recipient Organisation* endpoint to establish the report destination.
2. The *SIL* responds with the endpoint and the preferred method of delivery to allow storage of the report with an Intermediary before it is forwarded to the *Pathology Report Recipient Organisation* when they next connect to the network (i.e. a 'store and forward' instance).
3. The *Pathology Provider* requests for the encryption details from the *NASH* to allow for encryption of the message with an approved certificate.
4. The *NASH* responds with the encryption details for the message.
5. The *Pathology Provider* distributes the encrypted Report Instance to the Intermediary for storage. The *Pathology Report Recipient Organisation* will collect the encrypted Pathology Result Report Instance later.
6. The *Pathology Provider* distributes a notification message to the *Intermediary Notification Storage* for collection by the *Pathology Report Recipient Organisation* to advise them of the location and status of the report.
7. The *Pathology Report Recipient Organisation* receives the notification from the notification store and uses it to find the Pathology Result Report Instance location.
8. The *Pathology Report Recipient Organisation* receives the Pathology Result Report Instance from the Intermediary store.
9. The *Pathology Report Recipient Organisation* sends a notification to the *Pathology Result Report Provider* to acknowledge the report has been successfully processed. This means that the report has been decrypted and its contents parsed.

2.2 Community Policies

This section lists the community policies that apply to the Pathology Result Report package, which can be viewed as requirements that are placed upon the package by government bodies and legislation.

A community policy constrains behaviour of one or more roles within a community. The Interoperability Framework defines three core policy types:

- *Obligations*, specifying required behaviour
- *Permissions*, specifying allowed behaviour
- *Prohibitions*, specifying forbidden behaviour.

These policies may influence the entire community, its internal processes, and/or its roles. A policy may directly influence some or all of the roles in an identical manner or influence different roles in different ways.

The purpose of this model is to provide a context which identifies the policy makers which have substantial influence over the community, and the policies they specify.

2.2.1 AS 4633-2004

NATA/RCPA supports AS 4633:2004: Medical laboratories - Particular requirements for quality and competence (ISO 15189) as the accreditation standard for assessments of medical laboratories from 1 July 2005 [NATA2005].

This standard outlines a number of specific obligations of a *Pathology Provider*, specifically in relation to reporting and communication. These include:

1. **Reporting of Results**, ensuring the establishment of critical/alert levels for all examinations and turnaround times which reflect clinical need
2. **Customer confidentiality**, ensuring there are policies and procedures to protect customers, including requirement regarding the electronic storage and transmission of results
3. **Control of Records**, ensuring appropriate records management procedures and measures to maintain record integrity.

2.2.2 Chain of Information Custody

Throughout the business service comprising the pathology process, the responsibilities of the Pathology Requester and Pathology Provider in ensuring the integrity and quality of the information transfer - at each stage of the Request-Test-Report Cycle - is termed 'Chain of Information Custody.' [RCPA2004]

The pathology process, in its simplest form, is shown in Figure 6.



Figure 6: The Pathology Process

2.2.2.1 The Pathology Process

The Pathology Process, in simplified form, is as follows:

1. A 'Requestor' can be a general practitioner that requests a pathology test to be performed
2. A 'Patient' is the subject that will provide the specimen for the pathology lab
3. 'Collection' involves the gathering of the specimen from the patient
4. 'Courier' involves the specimen being sent to the pathology provider
5. 'Registrar' represents a registered pathology laboratory that will perform the analysis
6. 'Analysis' is the actual process of examining the specimen and drawing a conclusion based upon the results
7. 'Consult' represents the validation of the results and, where required, consultation with peers
8. 'A Report' is the specific Pathology Result Report that is sent back to the Requestor or, in cases where a notifiable condition has appeared during testing, the report will also be sent to the required authorities
9. 'Account' involves the service costs and payments on the requestor account.

2.2.2.2 Pathology Provider

The Chain of Information Custody regarding the Report Stage states [RCPA2004] the following obligations on a reporting pathology provider:

1. The Pathology Provider is responsible for preparing and issuing to the Requester a comprehensive and clinically meaningful report of the outcomes of the pathology request.

2. In the case of screening programs the Pathology Provider must have systems in place to notify abnormal results to the Requester or their Nominated Delegate.
3. The issued report should meet NPAAC and NATA requirements, and include sufficient information for the Requester to optimise its value for patient care. The report should identify the original Requester and other practitioners who have been sent a copy of the report.
4. For Pathology Provider initiated tests, the Pathology Provider is responsible for communicating the results to the Requester or their Nominated Delegate.
5. The results should be transmitted in a timely and appropriate manner (hard-copy, electronic, verbal, etc) to the Requester or their Nominated Delegate.
6. Interim (hard-copy, electronic) reports should be clearly identified as such, and must be confirmed with a final report (hard-copy or electronic) that is clearly identified as such.
7. Telephone or other verbal reports are to be treated as interim reports and must be confirmed with a final report (hard-copy or electronic).
8. If an amended report is issued, it should be clearly identified as such. An amended report should indicate the information that has been amended, or alternatively be accompanied by the original report so that the Requester can readily identify the amended information.
9. For electronic delivery of reports the Pathology Provider should have mechanisms in place to record acknowledgement of receipt of report by the Requester or their Nominated Delegate.
10. The Pathology Provider should have in place a system to identify any requests that have not been responded to within the agreed time-frame. These reports should be prepared and issued with minimum further delay.
11. All electronic, verbal and hard copy communications between the Requester and the Pathology Provider related to pathology requests must be recorded in a suitable format and retained in accordance with relevant guidelines and regulations. NPAAC's Guidelines: Retention of Laboratory Records and Diagnostic Material currently recommend retaining the request, the laboratory records including records of analysis, calculations and observations from which the result is derived, and the report for a period of 3 years.
12. In appropriate cases, the Pathology Provider should notify the relevant authorities of notifiable diseases.
13. In cases where the Pathology Provider is unable to communicate life-threatening test results to the Requester or their Nominated Delegate in a clinically appropriate time frame, the Pathology Provider should endeavour to contact the patient, or their responsible carer as appropriate.

2.2.2.3 Pathology Report Recipient

Where the report is in response to a request the Chain of Information Custody also identifies the following obligations for the Pathology Report Recipient when they are the requester of the pathology services during the reporting stage:

1. The Requester (or their employing organisation) should have in place a management system to ensure that overdue or missing pathology reports are obtained, viewed and acted upon with minimum delay.
2. Where a Requester follows up a missing or overdue report and discovers that the patient has not been tested, the Requester should

endeavour to follow up the patient to discuss why they have not presented for the pathology test. The patient may require further information about the need for the test and what will take place. The Requester should document their discussions, and any written information provided to the patient.

3. The Requester should have a system in place to acknowledge the receipt of reports dispatched by the Pathology Provider.
4. In appropriate cases, the Requester should notify the relevant authorities of notifiable diseases.
5. Pathology reports should be retained as part of the patient record and in a readily retrievable secure format and environment.
6. All electronic, verbal and hard copy communications between the Requester and the Pathology Provider related to pathology reports must be recorded in a suitable format and retained in accordance with relevant guidelines and regulations. Data retention requirements will vary from State to State; however, the HIC currently recommends retaining the records for 18 months whilst medical indemnity organisations currently recommend retaining adult records for 7 years or for 7 years after the patient has turned 18.
7. As Requesters may not always be available to receive pathology reports. They should have in place a mechanism by which Pathology Providers can communicate unexpected life-threatening test results to the Requester or their Nominated Delegate in a clinically appropriate time-frame.

2.2.3 Requirements for Information Communication

NPAAC have published Requirements for Information Communication [NPAAC2007] which provides guidance to Pathology Providers as to the minimum standards for compliance with electronic messaging standards and security of messaging.

Specifically it states in S5.1, S5.2, and G6.1:

- To ensure the secure and confidential messaging of electronic pathology reports, laboratories must:
 - Ensure the completeness, accuracy and integrity of electronic messages (i.e. certainty that the message has not been altered during transmission)
 - Ensure the Pathology Provider message can be authenticated by the recipient
- 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
- Electronic communication of requests and reports should comply with protocols set out in the Standards Australia publications AS4700.2–2004 and HB262–2002 and their subsequent revisions.

2.2.4 Patient Identification

There is an *obligation* for *Pathology Providers* to have clear identification of individual patients in Pathology Reports. [NPAAC2007]

Most Pathology Providers will need to assign identifiers to individual patients to exercise this obligation and carry out their functions safely and efficiently in the best interests of the client. [NPAAC2007] This is consistent with those privacy laws which provide that individual identifiers should only be assigned

where reasonably necessary to enable the provider organisation to carry out its functions effectively.

The private sector and some State and Territory jurisdictions are prohibited from adopting Commonwealth Government identifiers (e.g., a Medicare number or a Veterans Affairs number) as their own identifiers except where such use has been authorised.

There are also restrictions on use and disclosure of Commonwealth identifiers. One of the exceptions is where it is necessary for the healthcare provider to fulfil their obligations to the Commonwealth agency. For example, a healthcare provider can collect a Medicare number to provide treatment under the Medicare Benefits Scheme (MBS) and then use or disclose the number to fulfil its MBS reporting obligations.

Some State and Territory laws also restrict adoption, use and disclosure of identifiers assigned by another State or Territory public sector organisation.

Patient identification in Pathology Reports would be facilitated by national unique patient identification. The UHI Services will incorporate an Individual Healthcare Identifier (IHI) for individuals. New legislation will need to be enacted before the UHI Services commences operation to address the existing legal barriers to adoption and handling of IHIs.

2.2.5 Provider Identification

There is an *obligation* for *Pathology Providers* to clearly identify the intended recipient of a Pathology Result Report [RCPA2004].

Identifying the recipient relates not only to the individual providers involved in the pathology communication process but also to the entity that the providers are employed by, or representing, in course of the transaction.

Amongst pathology organisations a variety of identifiers are currently used for provider identification, including name, local requesting system identifiers and local reporting system identifiers, among others.

In relation to funding, the Medicare Provider number is required to be used as the identifier for claiming purposes under the MBS [DOHA2005].

Provider identification would be facilitated by national unique provider identification. The UHI Services will incorporate a Healthcare Provider Identifier for Individuals (HPI-I) and a Healthcare Provider Identifier for Organisations (HPI-O). New legislation will need to be enacted before the UHI Services commences operation to address the existing legal barriers to adoption and handling of HPIs.

2.2.6 Information Privacy

Information privacy is a specific subset of 'privacy' and deals with the ways in which an individual's personal information may be collected and handled. Privacy-specific legislation and administrative instructions are the primary mechanisms for managing privacy within the health sector in Australia, although other legislation may contain specific provisions relating to the collection and handling of personal information [NEHTA2006].

Privacy legislation places obligations that affect all communications within the community. These obligations vary depending on the relevant regulatory scheme. Private sector healthcare providers are subject to the Commonwealth Privacy Act 1988 and may also be subject to state or territory privacy law. Public sector healthcare providers are subject to state or territory law with the exception of those in the Australian Capital Territory, who are subject to both Commonwealth and territory laws.

Nevertheless, the shared source of most Australian privacy legislation means that it is possible to extract a common set of privacy principles for the handling of health information.

In NEHTA's *Privacy Management Framework* [NPMF2008] the principles in the following table are addressed:

Privacy Principle		General Compliance Requirements
1	Collection	Collection is necessary; and Consent is obtained or collection authorised by or under law; and Individuals are notified of the collection.
2	Use and Disclosure Primary Purpose	Allowed.
	Use and Disclosure Secondary Purposes	Secondary purposes are directly related to primary purpose and within individual's reasonable expectations; or Consent is obtained; or Required or authorised by law; or Serious or imminent threat to any individual's life, health or safety.
3	Data Quality	Information is accurate, complete and up to date.
4	Data Security	Protection from misuse, loss and unauthorised access, and modification and disclosure; Destroy or de-identify information that is no longer necessary.
5	Openness	Provide a document that clearly sets out policies on handling personal information.
6	Access and Correction	On request and excluding certain circumstances, provide individuals with access to their personal and health information; Where reasonable, correcting health information at the request of the individual.
7	Identifiers	Assignment of identifiers must be necessary; Adoption of identifiers must be in accordance with prescribed circumstances.
8	Anonymity	Allow anonymity where lawful and practical.
9	Trans-border Data Flows	Transfer if reasonable belief recipient is subject to comparable information privacy scheme; or Transfer with individual's consent; or Transfer is necessary for contract at the request of, or to benefit the individual.

Table 1: NEHTA's Common Privacy Principles for the Collection and Handling of Health Information

The *Requirements for Information Communication* [NPAAC2007] contains more detailed national standards and guidelines concerning common privacy principles. These have been specifically developed to cover both public and private pathology providers. Where particularly relevant to pathology result reporting, NPAAC2007 standards and guidelines are extracted below or in the Implementation Guidelines.

In the absence of a single, coordinated national scheme regulating information privacy in Australia, this identification of common principles, standards and guidelines provides the best approach for the Pathology Result Reporting Package to identify privacy obligations. However, healthcare providers must ensure they comply with applicable Commonwealth, State and Territory legislation.

2.2.6.1 Use and Disclosure of Data

The *Requirements for Information Communication* [NPAAC2007] include the following standards and commentary with respect to use and disclosure of information:

- **S1.5** A laboratory [Pathology Provider] must not use or disclose an individual's health information, including results, except for the primary or directly related secondary purposes 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.
- **C1.5b** 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).
- **C1.5c** A directly related secondary purpose may include activities necessary for the proper functioning of the laboratory [Pathology Provider], and will usually be 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.
- **C1.5d** 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.

The further NPAAC2007 guidelines on use and disclosure for directly related and non-directly related secondary purposes include:

- **G1.9** 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 [Pathology Provider] 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 Security states Medical practitioners must take reasonable steps to protect the personal information they hold from misuse and loss and from unauthorised access, modification or disclosure and must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed.

This places an obligation on participants in the Pathology Reporting Community to secure information when in transit between parties.

2.2.6.2 Data Security

The *Requirements for Information Communication* [NPAAC2007] state, in relation to the Data security privacy principle that:

- **S1.8** The laboratory [Pathology Provider] must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

- **C.1.12** 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.

2.2.6.3 Requirements for Information Communication

Minimum standards for security of messaging are also provided at S5.1, S5.2 and G6.1, as outlined at 2.2.3 above.

The data security privacy principles and these standards place an obligation on participants in the Pathology Reporting Community to secure personal and health information.

2.2.6.4 Quality of Information

The *Requirements for Information Communication* [NPAAC2007] provide the following standard in relation to the data quality and correction of data privacy principle:

- **S1.6** The laboratory [Pathology Provider] 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.

In relation to Security of Data Management more generally (including access), NPAAC 2007 states that:

- **S4.1** Data must be managed to protect its integrity.
- **S4.2** Each laboratory [Pathology Provider] or laboratory network must identify at least one person whose role includes:
 - identifying, documenting and maintaining information about databases within the system (e.g. patients, referring doctors and laboratory staff)
 - ensuring that the system is available when required
 - ensuring that data are robust and reliable
 - identifying data retention periods
 - ensuring archived data are retrievable in a usable form
 - ensuring formal plans exist for the retiring or destruction of data and/or systems
 - 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.

As such an obligation exists that all communications within the community are to be conducted in a manner which upholds these standards.

2.2.6.5 Storage and Retention

Although not strictly applicable to the communication of information the storage and retention of artefacts created to facilitate communication is of concern to the Pathology Reporting Community.

Security of Storage is particularly important. The *Requirements for Information Communication* [NPAAC2007] state that:

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

- information is accessible only to authorised users
 - the integrity of information is maintained
 - the accuracy and completeness of information and processing methods is maintained
 - 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

As far as retention is concerned, the Requirements for Information Communication [NPAAC2007] state that:

- **S1.9** The laboratory [Pathology Provider] 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.
- **S1.10** The laboratory [Pathology Provider] must retain records according to the requirements in the appropriate NPAAC document addressing the retention of records and as required by relevant legislation.

All electronic, verbal and hard copy communications between the Pathology Report Recipient and the Pathology Provider related to Pathology Requests must be recorded in a suitable format and retained in accordance with relevant legislation, standards and guidelines.

Data retention requirements will vary from State to State, however, medical indemnity organisations currently recommend retaining records for 7 years for adults or in the case of minors, for 7 years after the patient turns 18 [RCPA2004].

In some circumstances the state provisions extend this to at least 10 years and for certain clinical areas such as Mental Health, records must be retained for lengthy periods such as 70 years or in some cases indefinitely.

NPAAC's Guidelines: Retention of Laboratory Records and Diagnostic Material currently recommend retaining the request, the laboratory records including records of analysis, calculations and observations from which the result is derived, and the report for a period of 3 years [NPAAC2002].

As such these Storage and Retention policies place obligations on the community to ensure that formats utilised for artefacts which require retention are secure, concise (i.e. lack redundancy), maintain usability (i.e. allow extraction of information) and retain readability for the life of the artefact.

3 Business Processes

This section describes the high level business processes in the Pathology Reporting Community occurring during the report exchange between the *Pathology Provider*, the *Intermediary* and the *Pathology Report Recipient*.

It provides background information on how reports are exchanged within the current scenario, known as the 'AS IS' business process.

3.1 Exchange Report

Within the Pathology Reporting Community the core process employed is Exchange Report, and is made up of nine distinct steps, each of which are business processes in their own right.

1. **Compile Report.** This process consolidates all the information for a pathology service request from different pathology tests and/or different pathology labs.
2. **Determine Receiver.** Each report will have one or more recipients, and this process collects the information about the recipients, their ability to receive reports, and also their preferred method of delivery.
3. **Distribute Reports.** This process sends the Pathology Result Report to the receiver via the requested method of delivery. The method of delivery is derived from the specified recipients of the Pathology Result Report, such that the report is delivered by one of two possible methods:
 - Manually via:
 - Fax
 - Australia post
 - Electronically via:
 - E-mail with an attached, encrypted PDF
 - Electronic Messaging.
4. **Construct Message.** Based upon the assumption that the message structure (not the report structure) varies between the Intermediary and Pathology Result Report Receiver, this process will format the message structure as appropriate.
5. **Sourcing Reports.** The process whereby the Pathology Report Recipient receives the report and makes the Pathology Provider aware of the fact, without the acknowledgment that the report is read and/or understood. The acknowledgement depends on the method of delivery.
6. **Acknowledgment Management.** This process provides feedback to the Pathology Provider on electronic processing of the report. This process is required due to legal requirements (see section community policies).
7. **Report Monitoring.** The process whereby the Pathology Provider checks to determine if the report has been read.
8. **Manage Report Storage.** The process whereby the Intermediary receives reports from Pathology Laboratories and stores the report until the request for retrieval from the Pathology Report Recipient is made.
9. **Report Pickup.** A manual process whereby the report is collected manually. This process is considered to be out of scope and is only mentioned for information purposes.

Figure 7 shows the 'AS IS' business process model, for the Exchange Report process.

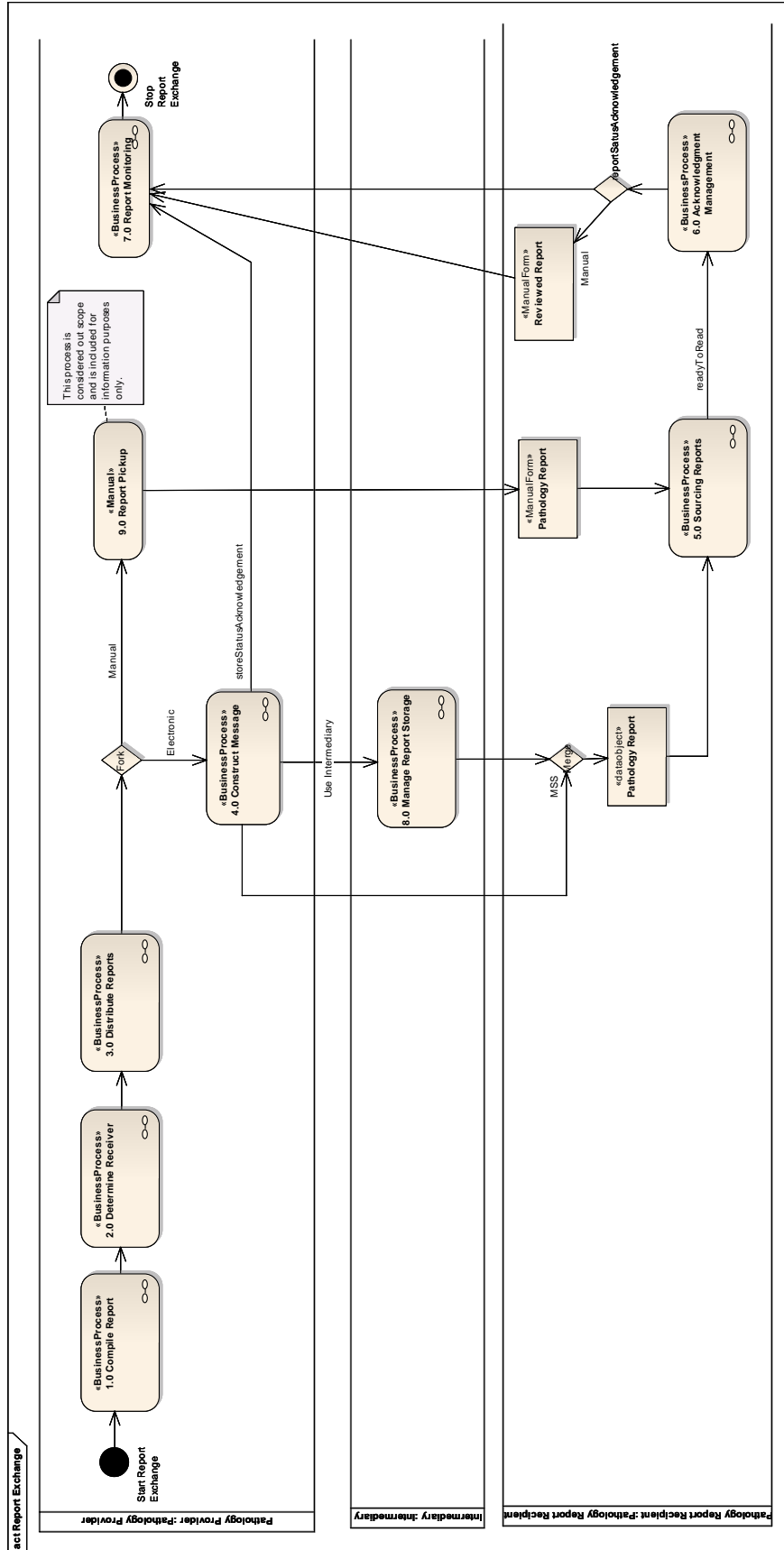


Figure 7: The 'AS IS' Business Process

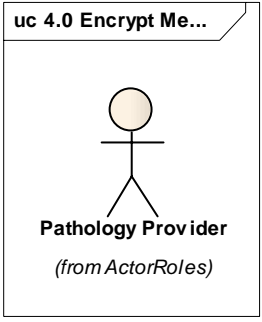
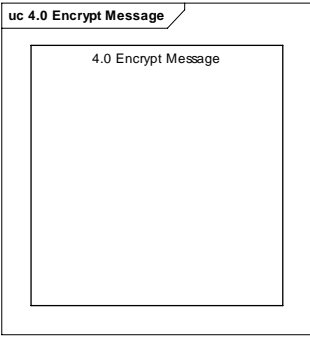
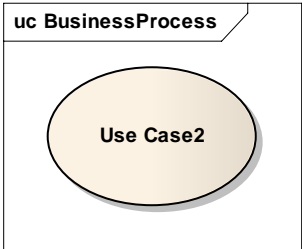

Business Process: Exchange Report	
Description	A high level business process description of the sending and receiving of a Pathology Result Report between the Pathology Provider, Intermediary and Pathology Report Recipient.
Actors/Roles	<ul style="list-style-type: none"> • Pathology Provider • Intermediary • A Pathology Report Recipient
Triggers	The tests and examinations on tissue and biopsy specimens is completed and a report is generated.
Precondition	The testing is completed and a report is required.
Main Success Scenario	<ol style="list-style-type: none"> 1. The <i>Pathology Provider</i> starts the 1.0 Compile Report process by collecting all the required report items and results. 2. The <i>Pathology Provider</i> starts the 2.0 Determine Receiver process collecting the Pathology Report Recipient details. 3. The <i>Pathology Provider</i> starts the 3.0 Distribute Reports process collecting the destination and method of delivery for the specified Pathology Report Recipient. <ol style="list-style-type: none"> a) Report will be distributed electronically. b) Report is to be delivered manually (alternate path) 4. The <i>Pathology Provider</i> will construct the appropriate message using the 4.0 Construct Message process and will send the report to: <ol style="list-style-type: none"> a) <i>Pathology Report Recipient</i> b) <i>Intermediary</i> (Alternate path) 5. The <i>Pathology Report Recipient</i> starts the 5.0 Sourcing Reports process allowing for the report to be received. 6. The <i>Pathology Report Recipient</i> notifies the Pathology Provider that the report is received, complete and understood by using the 6.0 Acknowledgement Management business process. 7. The <i>Pathology Provider</i> starts process 7.0 Report Monitoring to denote the end of service instance for this report. 8. Stop Main Success Scenario.
Post-Conditions	The <i>Pathology Report Recipient</i> has successfully received and understood the report and notified the Pathology Provider to close the service instance.

Business Process: Exchange Report	
Alternate Path	<p>3.b) The method of delivery is manual (the manual delivery of the report is not considered in scope of this document).</p> <ol style="list-style-type: none"> 1. Start Main Success Scenario step 5.0 Sourcing Reports. <p>4.b) The report is constructed for delivery to the <i>Intermediary</i>:</p> <ol style="list-style-type: none"> 1. The <i>Intermediary</i> uses the process 9.0 Manage Report Storage to allow for receiving the report from the Pathology Provider and to store the report until the Pathology Report Recipient requests for the report. (The request is initiated by the Pathology Request process, and is not in scope of this document.) 2. Start at step 5 of the Main Success Scenario. 3. Stop alternate path.
Policies	See section 2.2 Community Policies
Issues	<i>Pathology Report Recipients</i> do not have the capability to be connected to the network on a permanent basis; this causes delays in delivery of reports and restricts the ability for a fully-electronic solution.
Frequency	For each <i>Pathology Provider</i> service request.

4 Business Requirements

This section lists the functional and non-functional requirements from the Pathology Reporting point of view. It documents the 'TO BE' scenarios.

The following notations and descriptions are used for documenting the functional business requirements.

Notation	Description
	<p>The stick figure represents the actor. The actors are a classifier for entities (being humans or systems) outside the subject area, but interact directly with the subject.</p> <p>Actors are specified in primary and secondary actors, a primary actor has a direct interest in the result of the use case, and the secondary actor has a more indirect interest in the outcome and does not actively participate in the process [UMLRMV2].</p>
	<p>The subject boundary represented by a box around the use cases groups the uses cases into a system functionality area. It defines the system subject that is discussed. [UMLRMV2]</p> <p>Throughout the document the Business Process names introduced in section 4 are used to name the Subject Boundaries, giving the reader guidance on what Business Process in the Exchange Report Business Process Model are discussed.</p> <p>This approach is chosen to allow for quick identification of new and changed processes.</p>
	<p>Use Case notation, its purpose is to define a piece of behaviour without revealing the internal structure. The behaviour is described using Use Case "full dress" description. [UMLRMV2]</p>
	<p>Association shows relationship among two or more specified classifiers that describes connections among their instances. [UMLRMV2]</p>

Use Case: <i><name of the use case> as it can be understood by humans. We use a noun and a verb for defining a name that represents the Use Case function.</i>	
Description	Description of the use case in one paragraph or less.
Actors/Roles	The actors that are involved in the use case.
Triggers	What starts the use case.
Precondition	What conditions must be met before the use case is started.
Main Success Scenario	Also known as basic path, it outlines the steps the actor will take in normal conditions.

Use Case: <name of the use case> as it can be understood by humans. We use a noun and a verb for defining a name that represents the Use Case function.	
Post-Conditions	What is the end result of the use case?
Alternate Path	Provides alternates of the main success scenario, in general these are decisions points, in the context of this document, the error conditions are also described in the alternate path.
Extend	Must use one of the following use case(s) for support
Include	Must use the following use case(s)
Issues	Any issues relating to this use case.
Assumptions	Any assumptions made when writing this use case.

4.1 Functional

This section lists functional requirements, documented using the Unified Modelling Language (UML) approach and using the 'Full Dress' use case description to describe the functionality requirements.

4.1.1 1.0 Compile Report

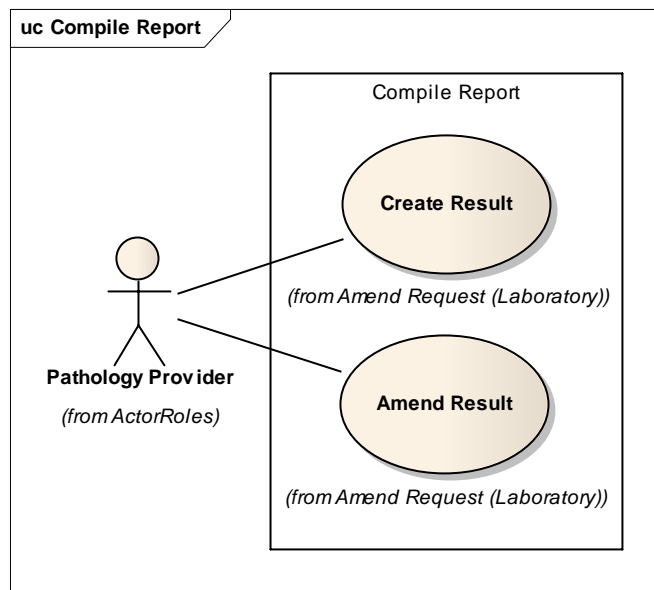


Figure 8: Use Case Diagram 1 – Compile Report

4.1.1.1 Requirement Reference

The requirement reference lists the origin of the requirements.

Requirement	Phase	Description
REQ001	1	A Pathology Result Report must utilise a standard reference terminology for clinical data elements contained within it.
REQ007	1	A Pathology Result Report must have clear identification of the patient that is the subject of the report.
REQ010	1	The Pathology Provider must prepare and issue a comprehensive and clinically meaningful Pathology Result Report detailing the outcomes of a pathology investigation.
REQ025	1	A Pathology Result Report shall contain the result(s) of the test(s) being reported.

Requirement	Phase	Description
REQ026	1	A Pathology Result Report shall contain the type of specimen on which the testing was performed.
REQ027	1	A Pathology Result Report shall contain the date and time (if appropriate) of specimen collection.
REQ028	1	A Pathology Result Report shall contain the quantitative or qualitative result for the test.
REQ029	1	A Pathology Result Report shall contain the units of measurement used to define the test result.
REQ030	1	A Pathology Result Report shall contain the age and gender related reference intervals if appropriate for the test result.
REQ031	1	A Pathology Result Report shall contain the identity of the laboratory or laboratory group which performed the test(s).
REQ032	1	A Pathology Result Report shall contain the requester and address(es) for delivery.
REQ033	1	A Pathology Result Report shall contain the identity of the laboratory or organisation issuing the report.
REQ034	1	A Pathology Result Report shall contain the name of the person responsible for the issued report.
REQ035	1	A Pathology Result Report shall contain a unique identifier of the correlating request.
REQ037	1	A Pathology Result Report shall contain a unique identifier for each instance of the report which is created by the Pathology Provider.
REQ038	1	A Pathology Result Report shall conform to the NPAAC and NATA requirements.
REQ046	1	Senders of Pathology Reports shall include clear identification of the intended recipient of any pathology report.
REQ049	1	The Pathology Result Report must indicate where the report has been created as a result of a Pathology Provider initiated test.
REQ086	1	A Pathology Report Recipient must provide a standard interface at a unique location through which it can receive Pathology Result Report Instances.
REQ205	1	If an amended Pathology Result Report is issued, it should be clearly identified as such.
REQ262	1	A Pathology Result Report Instance must be represented in a format conformant with the AS4700.2 HL7 V2.4; i.e a message with message type OUL^R21.

4.1.1.2 Community Policy Reference

The following policies (outlined in Chapter 2, Pathology Reporting Community) apply to this process:

- Pathology Provider - Section 2.2.2.2 – 2
- Pathology Provider - Section 2.2.2.2 – 3
- Requirements for Information Communication - Section 2.2.3 - S5.1
- Requirements for Information Communication - Section 2.2.3 - G6.1
- Information Privacy – Section 2.2.6 - NPP1, NPP2+10, NPP5, NPP6

The following external policies also apply to this process:

- NPAAC2007 S1.6
- RCPA 2004

4.1.1.3 Use Case: Create Result

This Use Case is detailed in the Pathology Result Reporting Package v1.0 – Structured Document Template. [PATH-PRR-SDT]

Use Case: Create Result	
Description	Information from the Pathology Provider information system is used in conjunction with Terminology to populate Data Elements as shown from the Pathology Result Report Structured Document Template to create one or more Results Reports from Pathology investigations.
Actors/Roles	Pathology Provider.
Triggers	The Pathology Provider completes Pathology testing and on a received specimen from the Subject of Care.
Precondition	The Pathology Provider information system is capable of creating electronic messages based on the Structured Document Template specifications with data populating the proposed Data Elements from their respective Data Groups together with approved Terminology.
Main Success Scenario	<ol style="list-style-type: none"> 1. The Pathology Provider created the report after the pathology test has been performed. 2. The Pathology Provider uses existing business processes to initiate a Pathology Result Report. 3. The Pathology Provider authorises the Pathology Result Report for distribution. 4. The Pathology Provider creates a message suitable for electronic communication, based on the Pathology Result Report Structured Document Template using data stored within the Laboratory Information System, together with approved terminology, populating data elements as specified in the Pathology Data Specification. 5. The electronic communication containing the Pathology Result Report is transferred to the Pathology Report Recipient. 6. End Use Case.
Post-Conditions	Compiled report as per specified standard. [PATH-PRR-SDT]
Alternate Path	None
Extend	Must use one of the following use case(s) for support: <ul style="list-style-type: none"> • None.
Include	Must use one of the following use case(s) for support: <ul style="list-style-type: none"> • None.
Issues	This use case is derived from the Structured Document Template – Pathology Result Report V1.0.

4.1.1.4 Use Case: Amend Result

This Use Case is detailed in the Pathology Result Reporting Package v1.0 – Structured Document Template. [PATH-PRR-SDT]

Use Case: Amend Result	
Description	Information from the Pathology Provider information system is use in conjunction with Terminology to populate Data Elements as shown from the Pathology Result Report Structure Document Template to amend one or more Results Reports from Pathology investigations.
Actors/Roles	Pathology Provider
Triggers	Results are amended by the Pathology Provider and required the information to be transferred to the Pathology Report Recipient.
Precondition	The Pathology Provider has the functionality to amend results and create amended information based on the Structure Document Template for Pathology Result Report and data (linked to terminology) contained with Data Elements from the Pathology Data Group.
Main Success Scenario	<ol style="list-style-type: none"> 1. The Pathology Provider amends the results on the Pathology Report. 2. The Pathology Provider creates an electronic message detailing the information. 3. End Use Case.
Post-Conditions	Amended Pathology Result report as per specified standard. [PATH-PRR-SDT]
Alternate Path	None
Extend	Must use one of the following use case(s) for support: <ul style="list-style-type: none"> • Create Result.
Include	Must use one of the following use case(s) for support: <ul style="list-style-type: none"> • None.
Issues	This use case is derived from the Structured Document Template – Pathology Result Report V1.0.

4.1.2 2.0 Determine Receiver

This process allows the Pathology Provider to find the location endpoint to which the Pathology Result Report must be distributed, on a systems level.

This process has the following functionality:

- *Determine Endpoint*, this function searches for the location endpoint
- *Determine Capability*, this function searches for the capability of the location endpoint, based on how the Pathology Result Report must be delivered to the Pathology Report Recipient.

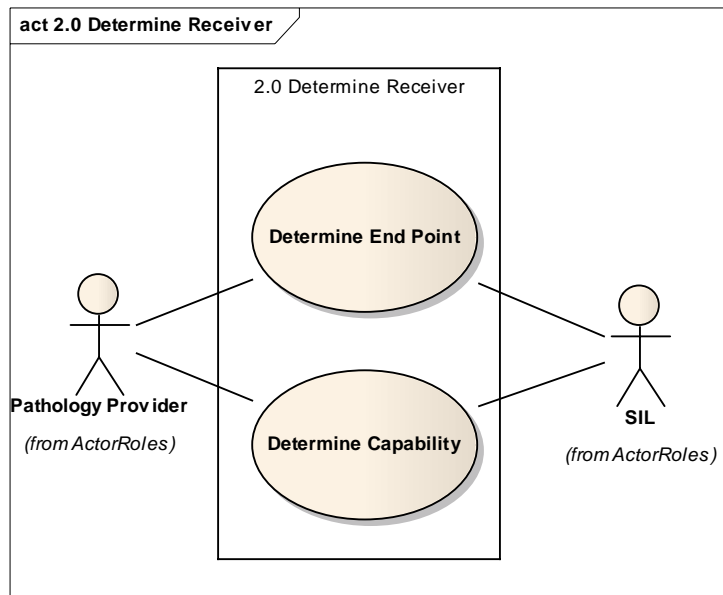


Figure 9: Use Case Diagram 9 – Determine Receiver

4.1.2.1 Requirement Reference

The requirement reference lists the origin of the requirements.

Requirement	Phase	Description
REQ111	1	Communications within the community should use HPI-O's for the unique identification of healthcare provider organisations.
REQ112	1	Communications within the community should use HPI-I's for the unique identification of healthcare provider individuals.
REQ118	1	Communications within the community should use IHI's for the unique identification of healthcare individuals.
REQ203	1	The Pathology Result Report should identify the original requester and other practitioners who have been sent a copy of the report.

4.1.2.2 Community Policy Reference

The following policies (outlined in Chapter 2, Pathology Reporting Community) apply to this process:

- Pathology Provider - Section 2.2.2.2 – 3
- Pathology Provider - Section 2.2.2.2 – 4
- Pathology Provider - Section 2.2.2.2 – 13

4.1.2.3 Use Case: Determine Endpoint

Use Case: Determine Endpoint	
Description	The destination must be known before a message can be sent from the Pathology Provider to either the Intermediary or the Pathology Report Recipient, the location of the service must be found.
Actors/Roles	<ul style="list-style-type: none"> • <i>SIL</i>, providing the location of the service. • <i>Pathology Provider</i> uses <i>SIL</i> to find the endpoint for the service for either the <i>Intermediary</i> or <i>Pathology Report Recipient</i>.
Triggers	The Pathology Provider completed the Pathology Result Report and is ready to distribute the report.
Precondition	The Pathology Result Report is completed and is ready for distribution.
Main Success Scenario	<ol style="list-style-type: none"> 1. The <i>Pathology Provider</i> contacts the <i>SIL</i> to determine the Endpoint of the service: <ol style="list-style-type: none"> a) <i>SIL</i> is available b) <i>SIL</i> is not available (Alternate Path). 2. The <i>Pathology Provider</i> must be successfully authenticated. 3. The <i>SIL</i> locates the Endpoint: <ol style="list-style-type: none"> a) Endpoint found b) Endpoint not found (Alternate path). 4. The <i>SIL</i> provided the endpoint to the Pathology Provider. 5. End Use Case.
Post-Conditions	The endpoint is successfully provided to the <i>Pathology Provider</i> .
Alternate Path	<p>1.b) <i>SIL</i> is not available</p> <ol style="list-style-type: none"> 1. The <i>Pathology Provider</i> contacts the <i>Pathology Report Recipient</i> manually to obtain the service endpoint. <p>3.b) Endpoint not found</p> <ol style="list-style-type: none"> 1. The <i>Pathology Provider</i> contacts the <i>Pathology Report Recipient</i> manually to obtain the service endpoint.
Extend	Must use one of the following use case(s) for support: <ul style="list-style-type: none"> • None.
Include	Must use the following use case(s): <ul style="list-style-type: none"> • Determine Receiver: Determine Capability
Issues	The <i>SIL</i> capability might not be available in the e-health community before the Pathology Community enables e-health capabilities.

4.1.2.4 Use Case: Determine Capability

Use Case: Determine Capability	
Description	Determines the means of delivery, by listing what the capabilities are of the Pathology Report Recipient to receive the Pathology Report.
Actors/Roles	<ul style="list-style-type: none"> • <i>Pathology Provider</i>, establishing how the report can be distributed to the <i>Pathology Report Recipients</i>. • <i>SIL</i>, providing information on how the <i>Pathology Report Recipient</i> can receive the report.
Triggers	The <i>Pathology Provider</i> is determined the endpoint for the <i>Pathology Report Recipient</i> .
Precondition	An entry for the endpoint must exist in the <i>SIL</i> database.
Main Success Scenario	<ol style="list-style-type: none"> 1. The <i>SIL</i> provides the method of delivery for the <i>Pathology Report Recipient</i> to the <i>Pathology Provider</i>. 2. End Use Case.
Post-Conditions	The Pathology Provider has gained enough information to determine the distribution method for delivering the report, as part of the Distribute Report process.
Alternate Path	None.
Extend	Must use one of the following use case(s) for support: <ul style="list-style-type: none"> • None
Include	Must use the following use case(s): <ul style="list-style-type: none"> • Determine Receiver: Determine Endpoint.
Issues	The SIL capability might not be available in the e-health community before the Pathology Community enables e-health capabilities.

4.1.3 3.0 Distribute Report

Distribute report process is executed by the Pathology Provider and interacts with processes within the Pathology Report Recipient or Intermediary.

Distribute Report has the following functionality:

- Delivery Method
- PUT Report
- Host Report
- PUT Pathology Notification

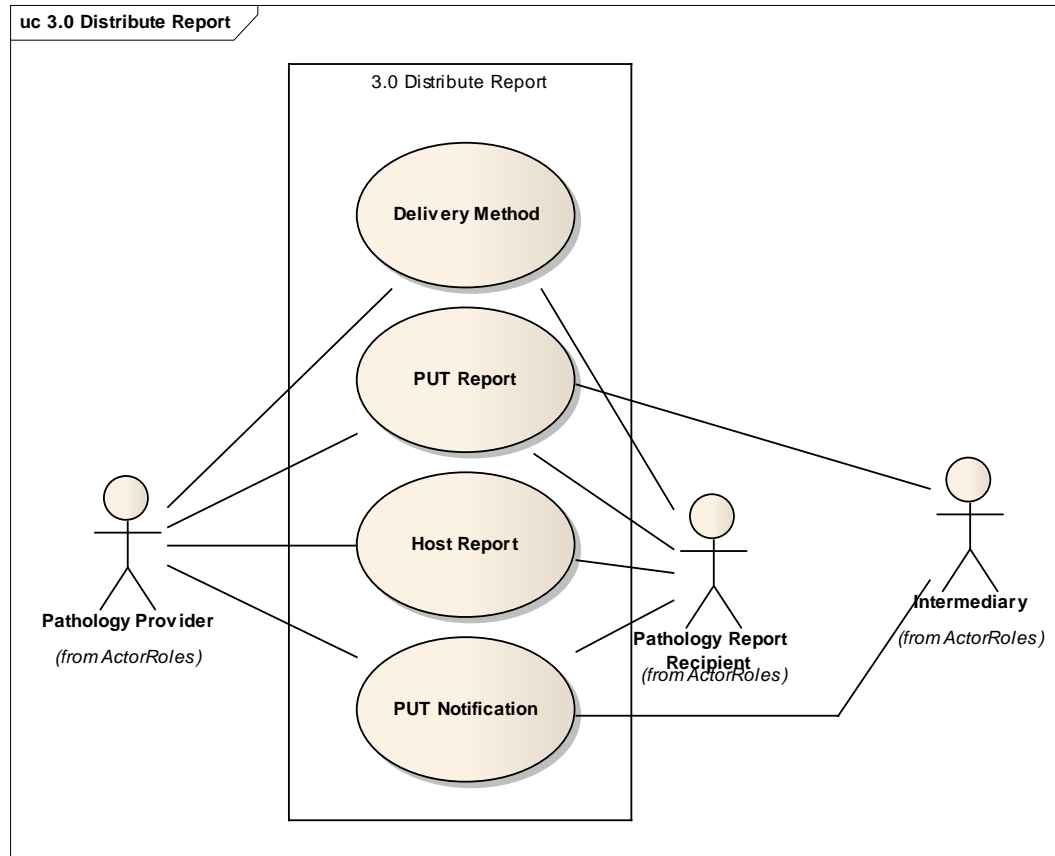


Figure 10: Use Case Diagram 3 – Distribute Report

4.1.3.1 Requirement Reference

The requirement reference lists the origin of the requirement.

Requirement	Phase	Description
REQ136	1	The <i>Pathology Provider</i> shall provide a mechanism for the transmission of reports to disconnected parties.
REQ089	1	The receiver (entity) shall send a response back to the sender (entity) when it is unable to correctly identify, authorise, authenticate or successfully exchange data.
REQ022	1	In cases where the <i>Pathology Provider</i> is unable to communicate life-threatening test results to the <i>Pathology Report Recipient</i> in clinically appropriate time frame alternative measures must be used.
REQ011	1	For the Reporting of Results, participants in the community must establish critical/alert levels for all examinations and turnaround times that reflect the clinical need.

4.1.3.2 Community Policy Reference

The following policies (outlined in Chapter 2, Pathology Reporting Community) apply to this process:

- AS 4633-2004 - Section 2.2.1 – 1
- Pathology Provider - Section 2.2.2.2 – 2
- Pathology Provider - Section 2.2.2.2 – 4
- Pathology Provider - Section 2.2.2.2 – 5
- Pathology Provider - Section 2.2.2.2 – 6
- Pathology Provider - Section 2.2.2.2 – 12
- Pathology Provider - Section 2.2.2.2 – 13
- Information Privacy – Section 2.2.6

The following external policies also apply to this process:

- AS4633-2004

4.1.3.3 Use Case: Delivery Method

Use Case: Delivery Method	
Description	This Use Case is to determine the method of report and notification delivery, for the Pathology Report Recipient.
Actors/Roles	<ul style="list-style-type: none"> • Pathology Report Recipient. • Pathology Provider.
Triggers	Report is ready for delivery.
Precondition	The method of delivery is known by the e-health community.
Main Success Scenario	<ol style="list-style-type: none"> 1. The <i>Pathology Provider</i> identifies the method of delivery: <ol style="list-style-type: none"> a) Electronic b) Manual (alternate path). 2. The <i>Pathology Provider</i> validates the <i>Pathology Report Recipient</i> method: <ol style="list-style-type: none"> a) Method is a PUT b) Method is a GET (alternate path). 3. The <i>Pathology Provider</i> starts the PUT Report Use Case. 4. End Use Case.
Post-Conditions	The <i>Pathology Provider</i> successfully PUT the report onto the Recipient location.
Alternate Path	<p>1b. Delivery method is manual.</p> <ol style="list-style-type: none"> 1. Manually notify the <i>Pathology Report Recipient</i> that the report is ready. 2. End Use Case <p>2b <i>Pathology Report Recipient</i> method is GET.</p> <ol style="list-style-type: none"> 3. The <i>Pathology Provider</i> starts the Host Report Use Case.

Use Case: Delivery Method	
Extend	<p>Must use one of the following use case(s) for support:</p> <ul style="list-style-type: none"> • Pathology Provider: PUT Report • Pathology Provider: Host Report • Pathology Provider: PUT Pathology Notification
Include	<p>Must use the following use case(s):</p> <ul style="list-style-type: none"> • Business process: Determine Receiver.
Issues	Some Pathology Report Recipients might only receive a hard copy of the report.
Assumptions	<ul style="list-style-type: none"> • Notifying the <i>Pathology Report Recipient</i> is a business process and is currently in place. • Reports send between <i>Pathology Report Recipients</i> is done via a <i>Pathology Provider</i>. • <i>SIL</i> will be used to identify the <i>Pathology Report Recipients</i> and <i>Intermediary</i>. • <i>Pathology Providers</i> can send reports between them without using an <i>Intermediary</i>.

4.1.3.4 Use Case: Host Report

Use Case: Host Report	
Description	<p>Only owned by the <i>Pathology Provider</i> and allows for the <i>Pathology Report Recipient</i> to collect the report directly from the <i>Pathology Provider</i>.</p> <p>The Host Report Use Case is unique for the <i>Pathology Provider</i>.</p>
Actors/Roles	<ul style="list-style-type: none"> • <i>Pathology Report Recipient</i>, retrieving the report from the hosted location after initiating Get Report. • <i>Pathology Provider</i>, hosting the report location and if required PUT a report into the host location using PUT Report.
Triggers	The Delivery Method Use Case.
Precondition	<p>The Delivery Method Use Case determined that the report needs to be hosted locally to allow a <i>Pathology Report Recipient</i> to collect the report.</p> <p>The PUT Report process was completed successfully.</p>
Main Success Scenario	<ol style="list-style-type: none"> 1. The <i>Pathology Provider</i> receives a GET report request from <i>Pathology Report Recipient</i>. 2. The <i>Pathology Report Recipient</i> must be successfully authenticated. 3. The <i>Pathology Provider</i> must only lists the available pathology reports for the authorised <i>Pathology Report Recipient</i>. 4. The <i>Pathology Report Recipient</i> retrieves the selected report. 5. End Use Case.
Post-Conditions	The report is successfully hosted by the <i>Pathology Provider</i> and can be collected by the <i>Pathology Report Recipient</i> .
Alternate Path	None

Use Case: Host Report	
Extend	<p>Must use one of the following use case(s) for support:</p> <ul style="list-style-type: none"> • <i>Pathology Report Recipient</i>: Get Report • <i>Pathology Provider</i>: PUT Report
Include	<p>Must use the following use case(s):</p> <ul style="list-style-type: none"> • Security Management: Authenticate Credentials • Security Management: Authorise Access
Issues	<p>Some <i>Pathology Report Recipients</i> might only receive a hard copy of the report.</p>
Assumptions	<ul style="list-style-type: none"> • Report sent between <i>Pathology Report Recipients</i> is done via a <i>Pathology Provider</i>. • <i>Pathology Providers</i> can send reports between them without using an <i>Intermediary</i>. • <i>Pathology Providers</i> encrypt the report when the PUT Report process is executed. • Providing the credentials as part of the ability to authenticate and authorise is included in the Security Management. • The <i>Pathology Provider</i>: PUT Report process notifies the <i>Pathology Report Recipient</i> that a report is available.

4.1.3.5 Use Case: PUT Report

Use Case: PUT Report	
Description	<p>This is the process allowing the <i>Pathology Provider</i> to PUT a report onto a <i>Intermediary</i> or <i>Pathology Report Recipient</i> location.</p>
Actors/Roles	<ul style="list-style-type: none"> • <i>Pathology Report Recipient</i>, always online and opted for PUT report. In future releases the recipient in this scenario can also be a <i>Pathology Provider</i>. • <i>Pathology Provider</i>, putting the report. • <i>Intermediary</i>, functioning as a storage place for the report to allow for collection by the <i>Pathology Report Recipient</i> at a later stage.
Triggers	<p>The need to store a report in at a location to allow for retrieval by the <i>Pathology Report Recipient</i>.</p>
Precondition	<p>The <i>Pathology Report Recipient</i> opted for an electronic and direct PUT transfer mechanism and the <i>Pathology Report Recipient</i>: Receive Item process is available.</p> <p>The <i>Pathology Report Recipient</i> is successfully identified in 2.0 Determine Receiver.</p>
Main Success Scenario	<ol style="list-style-type: none"> 1. The <i>Pathology Provider</i> PUT the report on: <ol style="list-style-type: none"> a) An <i>Intermediary</i> storage. b) <i>Pathology Report Recipient</i> location (Alternate Path) c) Hosted location. 2. The <i>Pathology Provider</i> must encrypt the data

Use Case: PUT Report	
	<p>using the Secure Data Use Case.</p> <ol style="list-style-type: none"> 3. The <i>Intermediary</i> must be successfully authenticated. 4. The <i>Pathology Provider</i> PUT the report at the Intermediary location. 5. The <i>Pathology Provider</i> must validate that the PUT is: <ol style="list-style-type: none"> a) Successful b) Unsuccessful (Alternate Path) 6. The <i>Pathology Provider</i> starts the PUT Pathology Notification Use Case. 7. End Use Case.
Post-Conditions	The <i>Pathology Provider</i> successfully PUT the report onto the <i>Intermediary</i> location.
Alternate Path	<p>1.b)1 <i>Pathology Provider</i> PUT the report on a Pathology Report Recipient location.</p> <ol style="list-style-type: none"> 1. The <i>Pathology Report Recipient</i> must be successfully authenticated. 2. The <i>Pathology Provider</i> PUT the Pathology Result Report at the Pathology Recipient location. 3. The <i>Pathology Provider</i> must validate that the PUT is: <ol style="list-style-type: none"> a) Successful b) Unsuccessful (Alternate Path) <p>1.c) <i>Pathology Provider</i> PUT the report on a Host location.</p> <ol style="list-style-type: none"> 1. The <i>Pathology Provider</i> must encrypt the data. 2. The hosting location must be successfully authenticated. 3. The <i>Pathology Provider</i> PUT the report at the Host location. 4. The <i>Pathology Provider</i> must validate that the PUT is. <ol style="list-style-type: none"> a) Successful b) Unsuccessful (Alternate Path) 5. The Pathology Provider starts the PUT Pathology Notification Use Case. <p>3.b). The <i>Pathology Provider</i> validated that the PUT was not successful.</p> <ol style="list-style-type: none"> 1. The <i>Pathology Provider</i> must manually notify the <i>Pathology Report Recipient</i>. 2. End Alternate Path.
Extend	<p>Must use one of the following use case(s) for support:</p> <ul style="list-style-type: none"> • <i>Pathology Report Recipient</i>: Receive Report • <i>Pathology Provider</i>: Host Report

Use Case: PUT Report	
	<ul style="list-style-type: none"> • <i>Intermediary</i>: Store Report
Include	<p>Must use the following use case(s):</p> <ul style="list-style-type: none"> • Security Management: Authenticate Credentials • Security Management: Authorise Access • Security Management: Secure Data
Issues	<ol style="list-style-type: none"> 1. The responsibility of the <i>Pathology Provider</i> to PUT the report stops when the Pathology Result Report is successfully delivered to either the <i>Intermediary</i> and/or the <i>Pathology Report Recipient</i>. This does not include the validation of the data or validation that the end receiver of the Pathology Result Report can actually read the report. 2. The <i>Intermediary</i> is not considered to be a trusted party; this implies that the Pathology Result Report content must be encrypted to prevent the <i>Intermediary</i> reading the Pathology Result Report content.
Assumptions	<ul style="list-style-type: none"> • This process applies to permanent connected <i>Pathology Report Recipient</i>. • Reports send between <i>Pathology Report Recipients</i> is done via a <i>Pathology Provider</i>: PUT Report Process. • SIL will be used to identify the: <ul style="list-style-type: none"> – <i>Pathology Report Recipient</i>. – <i>Pathology Result Report Provider</i>, when they act as a report recipient. – <i>Intermediary</i>. • The <i>Intermediary</i> can act on behalf of the <i>Pathology Report Recipient</i> with respect to receiving the report. • If the <i>Pathology Report Recipient</i> (receiving party) cannot be contacted the report will be considered to be unsent.

4.1.3.6 Use Case: PUT Notification

Use Case: PUT Notification	
Description	This process is to allow the Pathology Provider to send a notification to the Pathology Recipient that a report is ready for collection or delivery.
Actors/Roles	<ul style="list-style-type: none"> • <i>Pathology Provider</i>, to compile and distribute the notification to the receiver. • <i>Pathology Report Recipient</i>, end-user of the notification. • <i>Intermediary</i>, storing the notification for future collection.
Triggers	The <i>Pathology Provider</i> identified that a <i>Pathology Report Recipient</i> opted to receive a notification.
Precondition	<i>Pathology Report Recipient</i> opted for a notification to be put at their location.

Use Case: PUT Notification	
Main Success Scenario	<ol style="list-style-type: none"> 1. The <i>Pathology Provider</i> constructs the notification for the <i>Pathology Report Recipient</i>. <ol style="list-style-type: none"> a) Must include <i>Pathology Provider</i> identity. b) Must include <i>Pathology Report Recipient</i>. c) Must include Pathology Result Report identity. d) Must include size (Kb). e) Must include date and time stamp. f) Must include Pathology Result Report host or store location. 2. The <i>Pathology Provider</i> PUT the notification on a: <ol style="list-style-type: none"> a) Notification Store. b) <i>Pathology Report Recipient</i> (alternate path) 3. The <i>Intermediary</i> must be successfully authenticated. 4. The <i>Pathology Provider</i> PUTs the notification at the <i>Intermediary</i> location. 5. The <i>Pathology Provider</i> must validate that the PUT is. <ol style="list-style-type: none"> a) Successful b) Unsuccessful (Alternate Path) 6. End Use Case.
Post-Conditions	The <i>Pathology Provider</i> successfully PUT the notification onto the <i>Intermediary</i> location.
Alternate Path	<p>2.b) <i>Pathology Provider</i> PUT the notification on a Pathology Report Recipient location.</p> <ol style="list-style-type: none"> 1. The <i>Pathology Report Recipient</i> must be successfully authenticated. 2. The <i>Pathology Provider</i> must PUT the notification at the Pathology Recipient location. 3. Start Main Success Scenario step 6. 4. End Alternate Path. <p>5.b) The <i>Pathology Provider</i> validated that the PUT was not successful.</p> <ol style="list-style-type: none"> 1. The <i>Pathology Provider</i> must manually notify the <i>Pathology Report Recipient</i>. 2. End Alternate Path.
Extend	Must use one of the following use case(s) for support: <ul style="list-style-type: none"> • <i>Pathology Report Recipient</i>: Receive Item • <i>Intermediary</i>: Store Notifications
Include	Must use the following use case(s): <ul style="list-style-type: none"> • Security Management: Authenticate Credentials • Security Management: Authorise Access • <i>Pathology Provider</i>: PUT Report
Issues	Some <i>Pathology Report Recipients</i> might only receive a

Use Case: PUT Notification	
	hard copy of the report.
Assumptions	<ul style="list-style-type: none"> • Notifying the <i>Pathology Provider</i> is a business process and is currently in place. • Reports send between <i>Pathology Report Recipients</i> is done via a <i>Pathology Provider</i>. • <i>SIL</i> will be used to identify the <i>Pathology Report Recipients</i>, <i>Pathology Provider</i> and <i>Intermediary</i>. • <i>Pathology Providers</i> can send notifications between them without using an <i>Intermediary</i>. • Notifications are not encrypted. • Notifications can only be deleted by the original <i>Pathology Report Recipient</i>.

4.1.4 4.0 Encrypt Message

This process is executed when the *Pathology Provider* distributes the message to the *Pathology Report Recipient* and/or the *Intermediary*.

Encrypt Message has the following functionality:

- *Confidentiality Check*, this function checks what level of encryption is required for the payload.
- *Get Certificate*, this function collects the encryption details from NASH to allow for encryption so that only the *Pathology Report Recipient* can decrypt the Report.

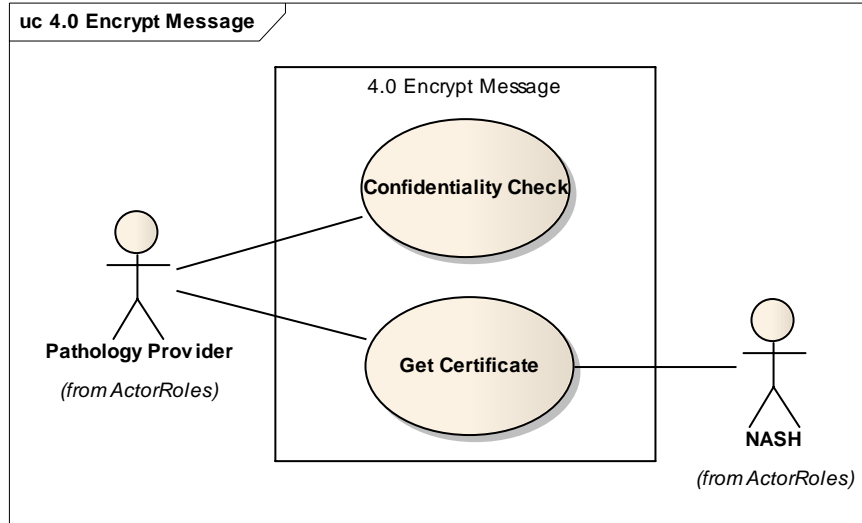


Figure 11: Use Case Diagram 4 – Encrypt Message

4.1.4.1 Requirement Reference

The requirement reference lists the origin of the requirement.

Requirement	Phase	Description
REQ18	1	Results should be transmitted in a timely and appropriate manner to the Pathology Report Recipient
REQ169	1	Credentials used for signing, encrypting and decrypting communications within the community must be X.509 V3 certificates

4.1.4.2 Community Policy Reference

The following policies (outlined in Chapter 2, Pathology Reporting Community) apply to this process:

- AS 4633-2004 - Section 2.2.1 – 1
- Pathology Provider - Section 2.2.2.2 – 2
- Requirements for Information Communication - Section 2.2.3 - S5.2

The following external policies also apply to this process:

- AS4633-2004
- RCPA2004 - NPP4

4.1.4.3 Use Case: Confidentiality Check

Use Case: Confidentiality Check	
Description	This function checks the type of payload and the confidentiality classification that is attached to it.
Actors/Roles	Pathology Provider
Triggers	The <i>Pathology Provider</i> constructed a report or notification that is ready for distribution using the e-health infrastructure.
Precondition	The Pathology Result Report is completed and is ready for distribution.
Main Success Scenario	<ol style="list-style-type: none"> 1. The <i>Pathology Provider</i> checks if the payload has: <ol style="list-style-type: none"> a) Patient data b) No patient data (Alternate Path) 2. The <i>Pathology Provider</i> determines that encryption is required. 3. The <i>Pathology Provider</i> starts use case Get Certificate. 4. End Use Case
Post-Conditions	Successfully established if there is patient data or not in the payload of the message.
Alternate Path	1.b) No patient data <ol style="list-style-type: none"> 1. The <i>Pathology Provider</i> determined that no encryption is required. 2. End Use Case
Extend	Must use one of the following use case(s) for support: <ul style="list-style-type: none"> • None
Include	Must use the following use case(s): <ul style="list-style-type: none"> • None
Issues	

4.1.4.4 Use Case: Get Certificate

Use Case: Get Certificate	
Description	This function collects the <i>Pathology Report Recipient</i> and if required the Intermediary certificate from NASH to allow encryption to occur.
Actors/Roles	<ul style="list-style-type: none"> • NASH Client • NASH
Triggers	Encryption is required.
Precondition	The <i>Pathology Provider</i> has determined that the payload requires encryption.
Main Success Scenario	<ol style="list-style-type: none"> 1. The Pathology Provider checks if the payload will be delivered to: <ol style="list-style-type: none"> a) <i>Pathology Report Recipient</i> b) <i>Intermediary</i> (Alternate Path)

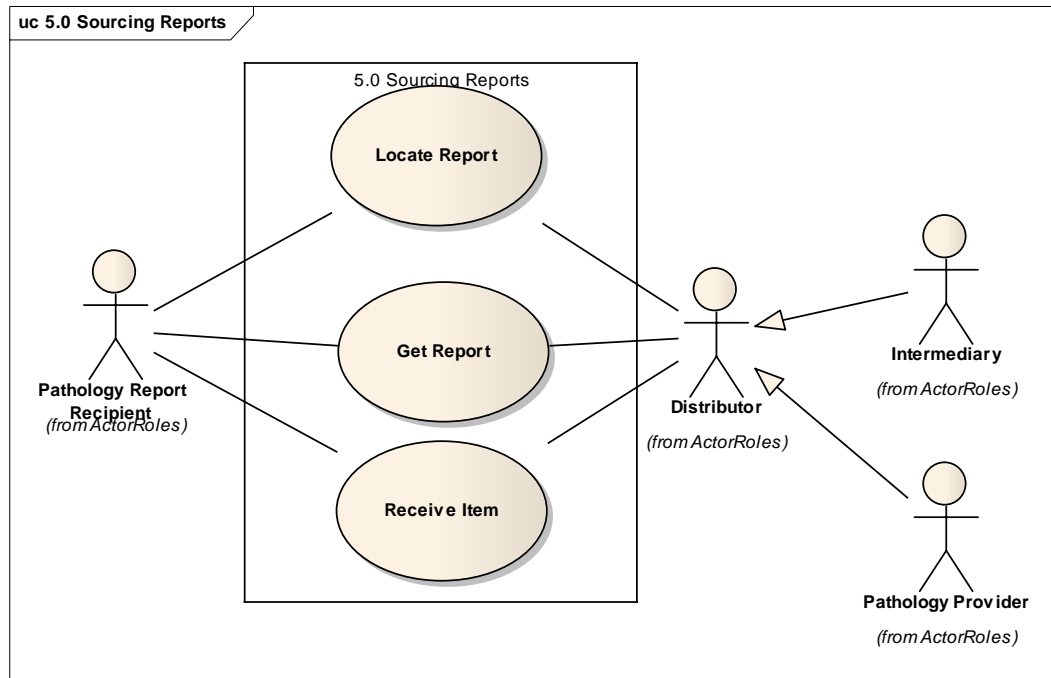
Use Case: Get Certificate	
	<ol style="list-style-type: none"> 2. The <i>Pathology Provider</i> contacts NASH 3. The Pathology Provider must be successfully authenticated. 4. The <i>Pathology Provider</i> requests the certificate from NASH for encryption. 5. NASH provides the encryption certificate. 6. End use case
Post-Conditions	The encryption certificate is successfully provided to the <i>Pathology Provider</i> .
Alternate Path	1.b) Intermediary <ol style="list-style-type: none"> 1. The Pathology Provider will query NASH once for the Pathology Report Recipient certificate and once for the Intermediary certificate. 2. End Use Case
Extend	Must use one of the following use case(s) for support: <ul style="list-style-type: none"> • <i>Pathology Provider</i>: Confidentiality Check • <i>Pathology Provider</i>: Determine Endpoint
Include	Must use the following use case(s): <ul style="list-style-type: none"> • None
Issues	

4.1.5 5.0 Sourcing Report

This process is executed by the *Pathology Report Recipient*, and allows for locating, getting and receiving reports from an *Intermediary* and/or *Pathology Provider*, both generalised as *Distributor* for this Use Case.

Sourcing Report has the following functionality:

- Locate Report
- Get Report
- Retrieve Item



4.1.5.1 Requirement Reference

The requirement reference lists the origin of the requirement.

Req. ID	Phase	Description
REQ023	1	The <i>Pathology Report Recipient</i> should have installed a management system to ensure that overdue or missing pathology reports are obtained, viewed and acted upon as quickly as possible.
REQ089	1	The receiver (entity) shall send a response back to the sender (entity) when unable to correctly identify, authorise, authenticate or successfully exchange data.
REQ094	1	A Report Responding System shall consider a Report Response to be undelivered until successful notification of delivery is received.

4.1.5.2 Community Policy Reference

The following policies (outlined in Chapter 2, Pathology Reporting Community) apply to this process:

- Pathology Provider - Section 2.2.2.2 – 3
- Pathology Provider - Section 2.2.2.2 – 4

4.1.5.3 Use Case: Locate Report

Use Case: Locate Report	
Description	<p>This is the process allowing the <i>Pathology Report Recipient</i>:</p> <ul style="list-style-type: none"> To locate a report identified within a notification. To locate a report identified as missing by the CIS To locate a report identified as over-due by the CIS
Actors/Roles	<ul style="list-style-type: none"> <i>Pathology Provider</i> and <i>Intermediary</i> generalised in Distributor. <i>Pathology Report Recipient</i>
Triggers	The need to find the location of the report.
Precondition	The <i>Pathology Report Recipient</i> needs to locate a report that is not received yet based upon the information they have available to them.
Main Success Scenario	<ol style="list-style-type: none"> The <i>Pathology Report Recipient</i> identifies the report ID. The <i>Pathology Report Recipient</i> identifies the Distributor of the report. The Distributor must be successfully authenticated. The <i>Pathology Report Recipient</i> checks availability. <ol style="list-style-type: none"> Distributor is available Distributor is not available (Alternate Path) Start use case: Get Report End Use Case
Post-Conditions	The <i>Pathology Report Recipient</i> is able to connect to the location where the report is distributed from.
Alternate Path	<p>4.b). Distributor is not available.</p> <ol style="list-style-type: none"> Manually notify the Distributor. End Use Case
Extend	<p>Must use one of the following use case(s) for support:</p> <ul style="list-style-type: none"> <i>Pathology Report Recipient</i>: Get Report
Include	<p>Must use the following use case(s):</p> <ul style="list-style-type: none"> Security Management: Authenticate Credentials Security Management: Authorise Access
Issues	
Assumptions	<ul style="list-style-type: none"> Notifying the <i>Pathology Provider</i> is a business process and is currently in place. Reports send between <i>Pathology Report Recipients</i> is done via a <i>Pathology Provider</i>. <i>SIL</i> will be used to identify the Distributor. Providing the credentials as part of the ability

Use Case: Locate Report	
	to authenticate and authorise is included in the Security Management.

4.1.5.4 Use Case: Get Report

Use Case: Get Report	
Description	Get report allows for the <i>Pathology Report Recipient</i> to initiate a report transmission from a Distributor.
Actors/Roles	<ul style="list-style-type: none"> • Distributor • <i>Pathology Report Recipient</i>
Triggers	Report location is known, and the <i>Pathology Report Recipient</i> is ready to get the report.
Precondition	<ul style="list-style-type: none"> • Distributor has capability available to allow for Get Report. • <i>Intermediary</i> this is Store Report. • <i>Pathology Provider</i> this is Host Report. • Notification is provided that there is a report available.
Main Success Scenario	<ol style="list-style-type: none"> 1. The <i>Pathology Report Recipient</i> determines the Distributor. <ol style="list-style-type: none"> a) <i>Intermediary</i> b) <i>Pathology Provider</i> (Alternate path) 2. The <i>Intermediary</i> must be successfully authenticated. 3. The <i>Intermediary</i> makes the report available. 4. The <i>Pathology Report Recipient</i> gets the report from the <i>Intermediary</i>. 5. The <i>Pathology Report Recipient</i> uses Report Receipt Acknowledgement to acknowledge the status of the report receipt. 6. End Use Case
Post-Conditions	The <i>Pathology Report Recipient</i> retrieves the report from the Distributor successfully.
Alternate Path	<p>1.b) the Distributor is a <i>Pathology Provider</i>.</p> <ol style="list-style-type: none"> 1. The <i>Pathology Provider</i> must be successfully authenticated. 2. The <i>Pathology Provider</i> makes the report available. 3. The <i>Pathology Report Recipient</i> gets the report from the <i>Pathology Provider</i>. 4. The <i>Pathology Report Recipient</i> uses Report Receipt Acknowledgement to acknowledge the status of the report receipt.
Extend	<p>Must use one of the following use case(s) for support:</p> <ul style="list-style-type: none"> • <i>Pathology Provider</i>: Host Report • <i>Intermediary</i>: Store Report • <i>Pathology Provider</i>: Report Receipt

Use Case: Get Report	
	<p>Acknowledgment.</p> <ul style="list-style-type: none"> • <i>Intermediary</i>: Store Notifications
Include	<p>Must use the following use case(s):</p> <ul style="list-style-type: none"> • Security Management: Authenticate Credentials. • Security management: Authorise Access.
Issues	<p>Some <i>Pathology Report Recipients</i> might only receive a hard copy of the report.</p>
Assumptions	<ul style="list-style-type: none"> • This process only works for system to system interaction. • Providing the credentials as part of the ability to authenticate and authorise is included in the Security Management. • If the report is stored by a <i>Pathology Provider</i> than Host Report will be used to allow for a GET report. • If report is stored by an <i>Intermediary</i> than Store Report will be used to allow for a GET report. • <i>Pathology Provider</i>: Host Report caters for listing of the reports. • <i>Intermediary</i>: Store Report caters for listing of the reports.

4.1.5.5 Use Case: Receive Item

Use Case: Receive Item	
Description	<p>This is the process used to receive the report or notification from a distributing party that initiated a PUT report as part of their process.</p>
Actors/Roles	<ul style="list-style-type: none"> • Distributor • <i>Pathology Report Recipient</i>
Triggers	<p>The <i>Pathology Report Recipient</i> is ready to get the report.</p>
Precondition	<p>The <i>Pathology Report Recipient</i> is able to receive the report.</p>
Main Success Scenario	<ol style="list-style-type: none"> 1. The Distributor provides its credentials. 2. The Distributor must be successfully authenticated by the <i>Pathology Report Recipient</i>. 3. The Distributor puts the report at the <i>Pathology Report Recipient</i> location. 4. The <i>Pathology Report Recipient</i> uses Report Receipt Acknowledgement to acknowledge the status of the report receipt. 5. End Use Case
Post-Conditions	<p>The Distributor has put the report on the <i>Pathology Report Recipient</i> location.</p>
Alternate Path	<p>None, in the event that the put is not successfully</p>

Use Case: Receive Item	
	completed the Distributor will initiate an alternate path.
Extend	<p>Must use one of the following use case(s) for support:</p> <ul style="list-style-type: none"> • <i>Intermediary</i>: Store Notifications, to allow for notifications to be stored in the event the <i>Pathology Provider</i> is not connected. • <i>Pathology Provider</i>: Receive Acknowledgement
Include	<p>Must use the following use case(s):</p> <ul style="list-style-type: none"> • Security Management: Authenticate Credentials • Security Management: Authorise Access • <i>Pathology Provider</i>: Put Report
Issues	Some <i>Pathology Report Recipients</i> might only receive a hard copy of the report.
Assumptions	<ul style="list-style-type: none"> • This process only applies for non permanent connected parties. • This process only works for system to system interaction. • Providing the credentials as part of the ability to authenticate and authorise is included in the Security Management. • Notifying of an unsuccessful put is the responsibility of the sending party, being the Distributor.

4.1.6 6.0 Acknowledgement Management

Acknowledgement Management is the functionality that allows for acknowledgment of the reports between the *Pathology Report Recipient*, the *Pathology Provider* and the *Intermediary* in compliance with the policies and procedures.

Acknowledgement Management has the following functionality:

- Report Processed Acknowledgement

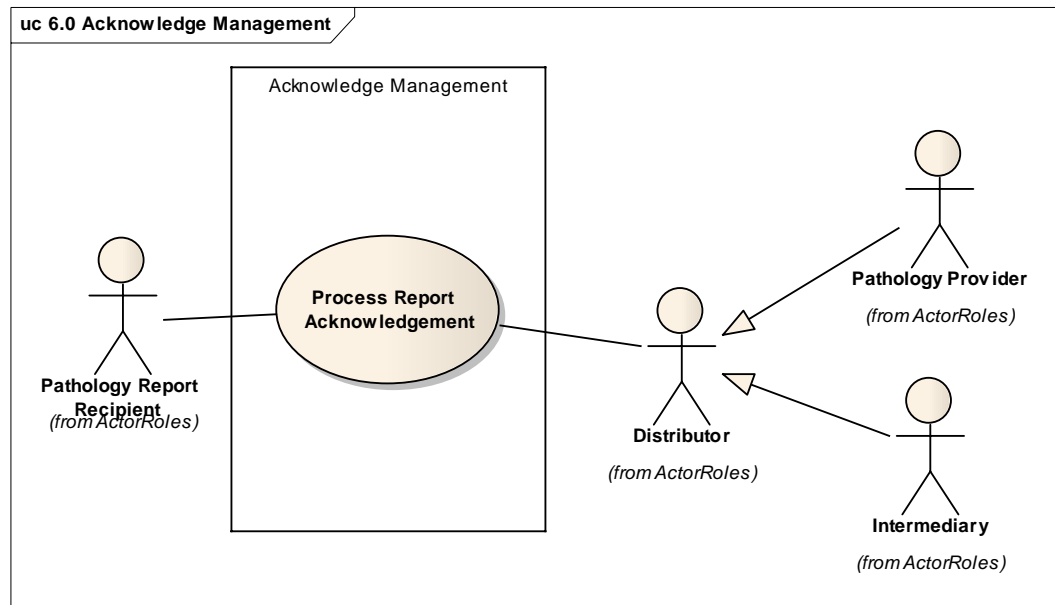


Figure 12: Use Case Diagram 6 – Acknowledgement Management

4.1.6.1 Requirement Reference

The requirements reference lists where the requirements originated from.

Req. ID	Phase	Description
REQ094	1	A Report Responding System shall consider a Report Response to be undelivered until successful notification of delivery is received by the sender of the report.
REQ051	1	<ul style="list-style-type: none"> • A response must be able to identify the sending and receiving entity. • A response shall contain the unique identifier of the payload instance as provided by the originator. • A response shall convey the outcome of the delivery to the sender and receiving entity. • A response shall indicate the date and time of the exchange to the sender and receiving entity. • A response must indicate the status of the data exchange. • A response must indicate the state of the payload being, received and processed.
REQ006	1	A Pathology Report Recipient must be able to identify and address a request for report dispatch to a Pathology Reporting System.

4.1.6.2 Community Policy Reference

The following policies (outlined in Chapter 2, Pathology Reporting Community) apply to this process:

- Requirements for Information Communication - Section 2.2.3 - S5.1

The following external policies also apply to this process:

- RCPA2004 - NPP4

4.1.6.3 Use Case: Report Processed Acknowledgement

Use Case: Report Processed Acknowledgement	
Description	This functionality allows for a response to be sent to the sender indicating that the report is successfully received by the <i>Pathology Report Recipient</i> .
Actors/Roles	<ul style="list-style-type: none"> • <i>Pathology Provider</i> and <i>Intermediary</i> generalised in Distributor. • <i>Pathology Report Recipient</i>.
Triggers	The Pathology Result Report is received from the <i>Pathology Provider</i> .
Precondition	The <i>Pathology Provider</i> requires an acknowledgement that the report is successfully processed by the <i>Pathology Report Recipient</i> .
Main Success Scenario	<ol style="list-style-type: none"> 1. The local system processes the Pathology Report. <ol style="list-style-type: none"> a) Processing is successful b) Processing is not successful (alternate path) 2. Acknowledge Message is generated. 3. The <i>Pathology Report Recipient</i> determines the Distributor requires a Report Receipt Acknowledgement. <ol style="list-style-type: none"> a) <i>Intermediary</i> b) <i>Pathology Provider</i> (Alternate path) 4. The <i>Intermediary</i> must be successfully authenticated. 5. The <i>Pathology Report Recipient</i> puts the notification using the Store Notification Use Case. 6. End Use Case.
Post-Conditions	An acknowledgement is created detailing the outcome of the processing and includes the credentials of the responding organisation for validation.
Alternate Path	<p>1.b) Processing is not successful</p> <ol style="list-style-type: none"> 1. Determine Pathology Result Report Sender 2. Acknowledge Message is generated 3. Start Main Success Scenario step 3. 4. End Alternate path. <p>3.b) The <i>Pathology Provider</i> needs a notification.</p> <ol style="list-style-type: none"> 1. The <i>Pathology Provider</i> must be successfully authenticated. 2. The <i>Pathology Report Recipient</i> puts the

Use Case: Report Processed Acknowledgement	
	notification using the Host Report use case. 3. End Use Case.
Extend	Must use one of the following use case(s) for support: <ul style="list-style-type: none"> <i>Intermediary</i>: Store Notifications, to allow for notifications to be stored in the event the <i>Pathology Provider</i> is not connected. <i>Pathology Provider</i>: Receive Acknowledgement
Include	Must use the following use case(s): <ul style="list-style-type: none"> Security Management: Authenticate Credentials Security Management: Authorise Access
Issues	Some <i>Pathology Report Recipients</i> might only receive a hard copy of the report.
Assumptions	<ul style="list-style-type: none"> The state of Processed or Process failure will relate to the successful or unsuccessful processing of a Pathology Result Report against the specified conformance criteria of well formed report. This process only works for system to system interaction. If the <i>Pathology Report Recipient</i> cannot process the report it is the recipient responsibility to escalate this to the <i>Pathology Provider</i>.

4.1.7 7.0 Report Monitoring

Report Monitoring is the functionality that allows for monitoring of the reports between the *Pathology Report Recipient*, the *Pathology Provider* and the *Intermediary*, in compliance with policies and procedures. Report Monitoring has the following functionality:

- Update Report Processed*, which updates the status of the report as successfully processed by the information system for the intended end user.

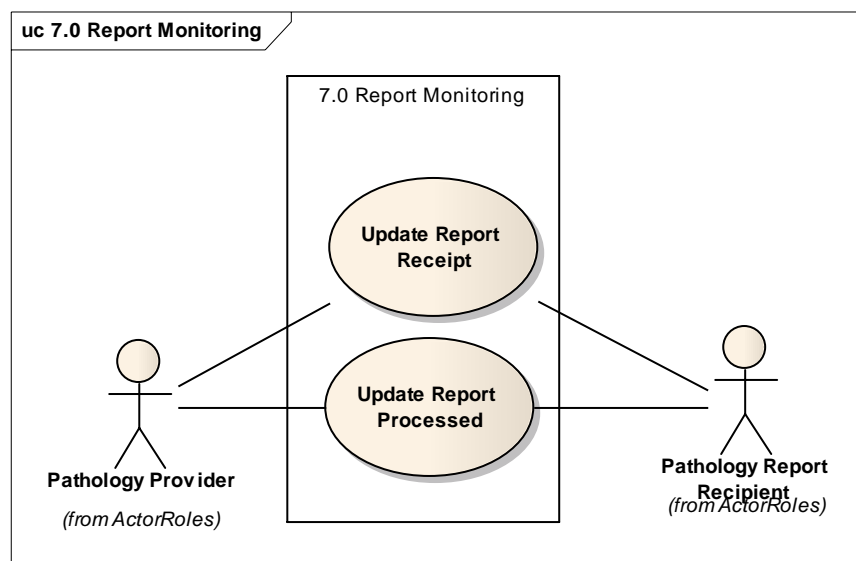


Figure 13: Use Case Diagram 7 – Report Monitoring

4.1.7.1 Requirement Reference

The requirements reference lists where the requirements originated from.

Req. ID	Phase	Description
REQ094	1	A Report Responding System shall consider a Report Response to be undelivered until successful notification of delivery is received by the sender of the report.
REQ051	1	<ul style="list-style-type: none"> • A response must be able to identify the sending and receiving entity. • A response shall contain the unique identifier of the payload instance as provided by the originator. • A response shall convey the outcome of the delivery to the sender and receiving entity. • A response shall indicate the date and time of the exchange to the sender and receiving entity.
REQ006	1	A <i>Pathology Report Recipient</i> must be able to identify and address a request for report dispatch to a Pathology Reporting System.
REQ013	1	For electronic delivery of reports the entities should have mechanisms in place to record acknowledgement, processing and error handling of the data exchange.
REQ021	1	A sender (entity) must be able to uniquely identify, locate, authorise and authenticate a recipient (entity) engaging in the data exchange service.
REQ104	1	Interim (hard-copy, electronic) reports should be clearly identified as such, and must be confirmed with a final report that is clearly identified as such.
REQ217	1	For <i>Pathology Provider</i> initiated tests, the <i>Pathology Provider</i> is responsible for communicating the results to the <i>Pathology Report Recipient</i> .
REQ220	1	Telephone or other verbal reports are to be treated as interim reports and must be confirmed with a physical final Pathology Report.

4.1.7.2 Community Policy Reference

The following policies (outlined in Chapter 2, Pathology Reporting Community) apply to this process:

- AS 4633-2004 – Section 2.2.1 – 3
- Pathology Provider – Section 2.2.2.2 – 1
- Pathology Provider – Section 2.2.2.2 – 2
- Pathology Provider – Section 2.2.2.2 – 3
- Pathology Provider – Section 2.2.2.2 – 5
- Pathology Provider – Section 2.2.2.2 – 6
- Pathology Provider – Section 2.2.2.2 – 7
- Pathology Provider – Section 2.2.2.2 – 9
- Pathology Provider – Section 2.2.2.2 – 10
- Pathology Provider – Section 2.2.2.2 – 11
- Requirements for Information Communication - Section 2.2.3 - S5.1

The following external policies also apply to this process:

- RCPA2004

4.1.7.3 Use Case: Update Report Processed

Use Case: Update Report Processed	
Description	<p>This function allows for the Report Processed Acknowledgment to be received by the <i>Pathology Provider</i>.</p> <p>The acknowledgement indicates that the report is processed by the <i>Pathology Report Recipient</i>.</p>
Actors/Roles	<ul style="list-style-type: none"> • <i>Pathology Report Recipient</i>, dispatching the Report Processed Acknowledgment. • <i>Pathology Provider</i>, receiving the Report Processed Acknowledgement and updating of the status.
Triggers	Pathology Result Report is successfully processed by the <i>Pathology Report Recipient</i> .
Precondition	The <i>Pathology Report Recipient</i> must be connected to the e-health network.
Main Success Scenario	<ol style="list-style-type: none"> 1. The <i>Pathology Provider</i> receives a Report Processed Acknowledge message. 2. The <i>Pathology Report Recipient</i> must be successfully authenticated. 3. The <i>Pathology Provider</i> validates the message. 4. The <i>Pathology Provider</i> processes the Report Receipt Acknowledgement and updates their systems with the status. 5. End use case.
Post-Conditions	The report receipt message is successfully received by the <i>Pathology Provider</i> .
Extend	
Include	
Issues	
Assumptions	<ul style="list-style-type: none"> • Currently there is a business process in place that supports acknowledgements. • Pathology Result Report status updates can be provided manually.

4.1.8 8.0 Manage Report Storage

Manage Report Storage is the functionality that allows for storage of the reports and notifications between the *Pathology Report Recipient* and the *Pathology Provider* in compliance with policies and procedures.

Manage Report Storage has the following functionality:

- Receive Report
- Store Report
- Store Notifications

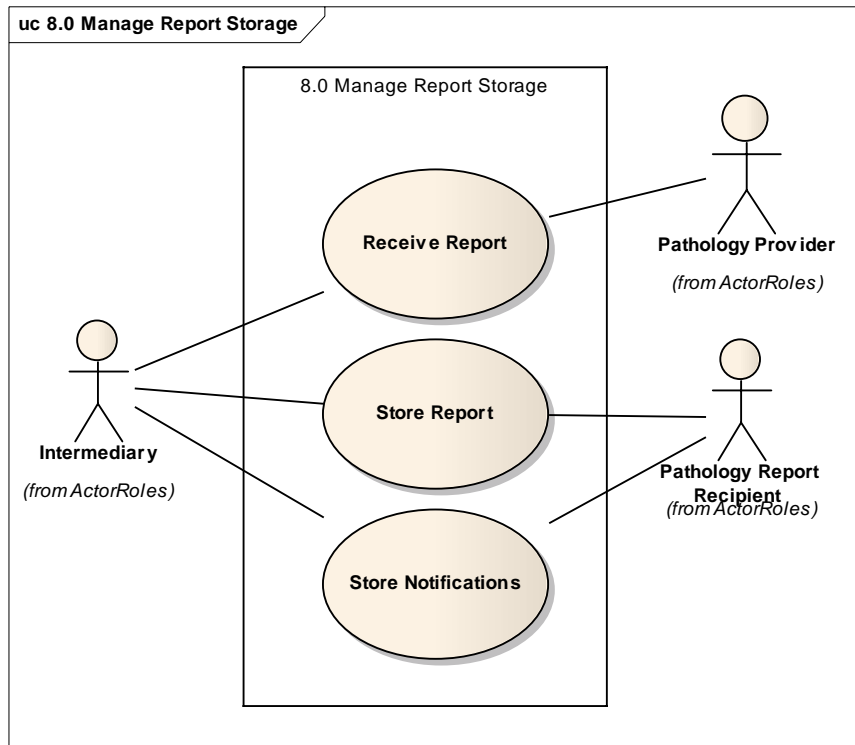


Figure 14: Use Case Diagram 8 – Manage Report Storage

4.1.8.1 Requirement Reference

The requirements reference lists where the requirements originated from.

Req. ID	Phase	Description
REQ136	1	The <i>Pathology Provider</i> shall provide a mechanism for the transmission of reports to disconnected parties.
REQ089	1	The receiver (entity) shall send a response back to the sender (entity) when unable to correctly identify, authorise, authenticate or successfully exchange data.
REQ022	1	In cases where the <i>Pathology Provider</i> is unable to communicate life-threatening test results to the <i>Pathology Report Recipient</i> alternative measures must be taken, within a clinically-appropriate time frame.

4.1.8.2 Community Policy Reference

The following policies apply to this process:

- None

4.1.8.3 Use Case: Receive Report

Use Case: Receive Report	
Description	Allowing the <i>Intermediary</i> to receive a report from the <i>Pathology Provider</i> .
Actors/Roles	<ul style="list-style-type: none"> • <i>Intermediary</i> • <i>Pathology Provider</i>
Triggers	Report location is known, and the <i>Pathology Report Recipient</i> is ready to get the report.
Precondition	<ul style="list-style-type: none"> • The Distributor passed Security Management. • The <i>Pathology Report Recipient</i> passed Security Management. • Report is available at the location.
Main Success Scenario	<ol style="list-style-type: none"> 1. The <i>Pathology Report Recipient</i> determines the Distributor. 2. The <i>Pathology Report Recipient</i> identifies themselves using its credentials. 3. The Distributor validates the <i>Pathology Report Recipient</i> credentials using Security Management. <ol style="list-style-type: none"> a) Validated successful. b) Validation failed (Alternate Path). 4. The Distributor identifies themselves using its credentials. 5. The Distributor makes the report available. 6. The <i>Pathology Report Recipient</i> validates the credentials using Security Management. <ol style="list-style-type: none"> a) Validated successful. b) Validation failed (Alternate Path). 7. The <i>Pathology Report Recipient</i> gets the report from the distributor. 8. End Use Case
Post-Conditions	The <i>Pathology Report Recipient</i> gets the report from the Distributor.
Alternate Path	<p>3.b) Validation failed</p> <ol style="list-style-type: none"> 1. Terminate connection 2. End Use Case <p>6.b) Validation failed</p> <ol style="list-style-type: none"> 1. Terminate connection 2. End Use Case
Extend	
Include	
Issues	Some <i>Pathology Report Recipients</i> might only receive a hard copy of the report.
Assumptions	<ul style="list-style-type: none"> • This process only applies for non permanent connected parties. • The actual processing of the report is existing functionality; this process only handles the

Use Case: Receive Report	
	<p>result of the report processing.</p> <ul style="list-style-type: none"> This process only works for system to system interaction.

4.1.8.4 Use Case: Store Report

Use Case: Store Report	
Description	This Use Case can only be used by the <i>Intermediary</i> and allows the <i>Pathology Report Recipient</i> to collect the report indirectly from the <i>Pathology Provider</i> .
Actors/Roles	<ul style="list-style-type: none"> <i>Pathology Report Recipient</i>, retrieving the report from the hosted location after initiating a GET. <i>Intermediary</i>, hosting the report location.
Triggers	Retrieval request from the <i>Pathology Report Recipient</i> .
Precondition	<ul style="list-style-type: none"> The <i>Pathology Report Recipient</i> is made aware of available reports, or initiates a report collection as part of its day to day business process. All Pathology Reports stored on the <i>Intermediary</i> location are encrypted.
Main Success Scenario	<ol style="list-style-type: none"> The <i>Intermediary</i> receives a GET report request. The <i>Pathology Report Recipient</i> must be successfully authenticated. The <i>Intermediary</i> must only list the available pathology reports for the authorised Pathology Report Recipient. The <i>Pathology Report Recipient</i> retrieves the selected report. End Use Case.
Post-Conditions	The report is successfully received by the <i>Pathology Report Recipient</i> .
Alternate Path	None
Extend	
Include	
Issues	<i>Intermediaries</i> are not a trusted source, however, they must be able to determine the <i>Pathology Report Recipient</i> so they can provide access to the report for download.
Assumptions	Reports send between <i>Pathology Report Recipients</i> is done via a <i>Pathology Provider</i> .

4.1.8.5 Use Case: Store Notifications

Use Case: Store Notifications	
Description	This process allows the <i>Pathology Provider</i> to send a notification to the <i>Pathology Report Recipient</i> that a

Use Case: Store Notifications	
	report is ready for collection or delivery.
Actors/Roles	<ul style="list-style-type: none"> • <i>Pathology Report Recipient.</i> • <i>Pathology Provider.</i> • <i>Intermediary.</i>
Triggers	The <i>Pathology Provider</i> identified that a <i>Pathology Report Recipient</i> opted to receive a notification.
Precondition	<i>Pathology Report Recipient</i> opted for a notification to be sent.
Main Success Scenario	<ol style="list-style-type: none"> 1. The <i>Pathology Provider</i> constructs the notification for the <i>Pathology Report Recipient</i>. <ol style="list-style-type: none"> a) Must include <i>Pathology Provider</i> identity. b) Must include <i>Pathology Report Recipient</i>. c) Must include Pathology Result Report identity. d) Must include date and time stamp. e) Must include Pathology Result Report host location. f) Must include expiry date. 2. The <i>Pathology Provider</i> PUTs the notification on a: <ol style="list-style-type: none"> a) Notification Store. b) <i>Pathology Report Recipient</i> (alternate path) 3. The <i>Intermediary</i> must be successfully authenticated. 4. The <i>Pathology Provider</i> PUTs the notification at the <i>Intermediary</i> location. 5. The <i>Pathology Provider</i> must validate that the PUT is. <ol style="list-style-type: none"> a) Successful b) Unsuccessful (Alternate Path) 6. End Use Case.
Post-Conditions	The <i>Pathology Provider</i> successfully PUT the notification onto the <i>Intermediary</i> location.
Alternate Path	<p>2.b) <i>Pathology Provider</i> PUT the notification on a <i>Pathology Report Recipient</i> location.</p> <ol style="list-style-type: none"> 1. The <i>Pathology Report Recipient</i> must be successfully authenticated. 2. The <i>Pathology Provider</i> PUTs the notification at the <i>Pathology Report Recipient</i> location. 3. Start Main Success Scenario step 5 4. End Alternate Path. <p>5.b) The <i>Pathology Provider</i> validated that the PUT was not successful.</p> <ol style="list-style-type: none"> 1. The <i>Pathology Provider</i> must notify the

Use Case: Store Notifications	
	<p><i>Pathology Report Recipient.</i></p> <p>2. End Alternate Path.</p>
Extend	<p>Must use one of the following use case(s) for support:</p> <ul style="list-style-type: none"> •
Include	<p>Must use the following use case(s):</p> <ul style="list-style-type: none"> • Security Management: Authenticate Credentials • Security Management: Authorise Access
Issues	<p>Some <i>Pathology Report Recipients</i> might only receive a hard copy of the report.</p>
Assumptions	<ul style="list-style-type: none"> • Notifying the <i>Pathology Provider</i> is a business process and is currently in place. • Reports send between <i>Pathology Report Recipients</i> is done via a <i>Pathology Provider</i>. • <i>SIL</i> will be used to identify the <i>Pathology Report Recipients</i>, <i>Pathology Provider</i> and <i>Intermediary</i>. • <i>Pathology Providers</i> can send reports between them without using an <i>Intermediary</i>.

Definitions

This section explains the specialised terminology used in this document.

Shortened Terms

This table lists abbreviations and acronyms in alphabetical order.

Term	Description
CC	Core Connectivity
CI	Clinical Information
CIS	Clinical Information System. The collaboration of computer systems and business processes with a common end goal; interoperable clinical information.
CT	Clinical Terminology
HPI	Healthcare Provider Identifier
HPI-I	Healthcare Provider Identifier – Individual
HPI-O	Healthcare Provider Identifier - Organisation
IEHR	Individual Electronic Health Record
ICT	Information and Communications Technology
IHI	Individual Healthcare Identifier
IHTSDO	International Health Terminology Standards Development Organisation
MRN	Medical Record Number
NASH	National Authentication Service for Health
NATA	National Association of Testing Authorities, functioning as Australia's national laboratory accreditation authority. http://www.nata.asn.au
NPAAC	National Pathology Accreditation Advisory Council http://www.health.gov.au/internet/main/publishing.nsf/Content/health-npaac-index.htm
PDI	NEHTA's Pathology Domain Initiative.
RCPA	The Royal College of Pathologists of Australia http://www.rcpa.edu.au/public/pathology/rcpa.cfm
SDT	Structured Document Template
SIL	Service Instance Locator
SNOMED CT	Systemised Nomenclature of Medicine, Clinical Terminology
TSIR	Technical Service Instance Record
UHI	Unique Healthcare identifiers
UML	Unified Modelling Language
UPI	Unique Patient Identifier

Glossary

This table lists specialised terminology in alphabetical order.

Term	Description
Activity	A business process (or single operation or step in a business process) performed by an entity as part of a greater system or behaviour.
Actor	Classifier for entities (Human, System) outside the subject that interacts directly with the subject. Actors are specified as primary and secondary actors. A primary actor has a direct interest in the results of a use case. A secondary actor has an indirect interest in the outcome, and does not actively participate in the process.
Alternate Path	If the main success scenario contains options, and one of those options is realised, then any subsequent steps are described in the alternate path. By branching the user away from the Main Success Scenario, the outcome of the use case may vary.
Business Architect	A Business Architect is anyone looks at the way work is being directed and accomplished, and then identifies, designs and oversees the implementation of improvements that are harmonious with the nature and strategy of the organisation. Source: http://www.businessarchitects.org
Business Requirements, Functional	Defines the requirements for the internal workings of the system, resulting from analysis and Use Case modelling.
Business Requirements, Non-Functional	Requirements that are not directly related to the internal workings of the system. Non-functional requirements may specify supporting items, including security, scalability and usability.
Business Service	Defined by the Interoperability Framework as a particular behaviour abstraction expressing the guarantees of service providers. The guarantees involve policies that apply to the service providers and, if a consumer accepts the service offer, other policies which are also applied to the consumer. This represents the formation of a service level agreement or a contract.
Community	A Community is defined as a collection of entities (e.g. individuals, organisations, information systems, resources, or various combinations of these), established to meet a given objective. [INTER2007]
Description	A paragraph explaining the purpose for a given Use Case.
Entity	An entity is a person or subject which can be uniquely identified in a particular context by a series of claims made about it. An entity does not have to have a physical form (e.g. a company). Entities may be identified using multiple identifiers, each with its own context and relevance.
Integrity	Refers to the preservation of data and the notion that it is guaranteed not to have been altered from its original meaning.
Intermediary	An entity that allows for storage of information (being Pathology Result Reports, Acknowledgments or Notifications) at other than the Pathology Provider or Pathology Report Recipient.
Interoperability	The ability of software and hardware on multiple machines from multiple vendors to communicate. Source: The Free On-line Dictionary of Computing. Denis Howe. 21 Apr. 2008. From: Dictionary.com - http://dictionary.reference.com/browse/Interoperability
Pathology Request	A referral for specialist pathology services.

Term	Description
Pathology Result Report	Represents a piece of structured, pathology related information including reports containing interim or final results, multimedia content, cumulative data such as significant result lists, outstanding requests or test reminder lists, among others.
Policy, Community	Constrains behaviour of one or more roles in a community, intended to address uncertainty in the community by increasing trust among actors/entities.
Role	A role specifies part of a community's structure and behaviour and can be fulfilled by different entities. Roles partition community structure and behaviour to reflect specific organisational arrangements.
System	<p>A collection of units (Human, System) organised to accomplish a purpose. A system can be described by one more models, possibly from different viewpoints. (A 'complete model' describes the whole system.)</p> <p>In this document the term does not directly relate to an IT system. The solution type documents will determine whether the system will be an ICT system or a human collaboration.</p>

References

This section lists NEHTA specifications and other documents that provide information for or about this document.

At the time of publication, the document versions indicated are valid. However, as all documents listed below are subject to revision, readers are encouraged to use the most recent versions of these documents.

Package Documents

The documents listed below are part of the suite delivered in the Pathology Result Reporting Package.

Discharge Summary Package Documents			
[REF]	Document Name	Publisher	Link
[PATH-PRR-CP]	Pathology Result Reporting Package v1.0 – Certification Procedures v1.0	NEHTA 2008	Reference in preparation for future release.
[PATH-PRR-EPS]	Pathology Result Reporting Package v1.0 – Endpoint Specification v2.0	NEHTA 2008	http://www.nehta.gov.au/ (Home > Publications)
[PATH-PRR-IA]	Pathology Result Reporting Package v1.0 – Information Architecture v2.0	NEHTA 2008	http://www.nehta.gov.au/ (Home > Publications)
[PATH-PRR-IG]	Pathology Result Reporting Package v1.0 – Implementation Guide	NEHTA 2008	Reference in preparation for future release.
[PATH-PRR-OCA]	Pathology Result Reporting Package v1.0 – Organisation Capability Assessment	NEHTA 2008	Reference in preparation for future release.
[PATH-PRR-PS]	Pathology Result Reporting Package v1.0 – Purpose and Scope v3.0	NEHTA 2008	http://www.nehta.gov.au/ (Home > Publications)
[PATH-PRR-RG]	Pathology Result Reporting Package v1.0 – Readers' Guide v3.0	NEHTA 2008	http://www.nehta.gov.au/ (Home > Publications)
[PATH-PRR-TA]	Pathology Result Reporting Package v1.0 – Technical Architecture v2.0	NEHTA 2008	http://www.nehta.gov.au/ (Home > Publications)

References

The documents listed below are non-package documents that have been cited in this document.

Reference Documents			
[REF]	Document Name	Publisher	Link
[DHS2005]	Medicare Australia, September 2005, Notice Information Technology Standards, DHS (accessed 2006-07-18)	DHS 2004	http://www.medicareaustralia.gov.au/provider/business/online/files/ma_notice_of_it_standards_electronic_and_paper_011005.pdf
[DOHA2004]	Department of Health and Ageing, September 2004, Medicare Statistics. 1984/85 to June Quarter 2004.	DOHA 2004	http://www.aodgp.gov.au/internet/main/publishing.nsf/Content/publications-Statistics
[DOHA2005]	Department of Health and Ageing, November 2005, Medicare Benefits Schedule, DOHA	DOHA 2005	http://www.aodgp.gov.au/internet/main/publishing.nsf/Content/publications-Statistics

Reference Documents			
[INTER2007]	Interoperability Framework, version 2.0, NEHTA, 2007.	NEHTA 2007	
[ICTS2004]	ICTSC, July 2004, Enabling e-Pathology Nationally, ICTSC	ICTS 2004	
[NATA2005]	National Association of Testing Authorities, April 2005, ISO 15189 - The New Standard for Medical Testing Laboratories, NATA	NATA 2005	
[NPAAC2002]	National Pathology Accreditation Advisory Council, 2002, Guidelines for Retention of Laboratory Records and Diagnostic Materials, Third Edition, accessed 2006-08-08,	NPAAC 2002	http://www.health.gov.au/internet/main/Publishing.nsf/Content/health-npaac-docs-retentionlab.htm
[NPAAC2006]	National Pathology Accreditation Advisory Council, 2006, Draft Standards for Pathology Laboratories,	NPAAC 2006	http://www.health.gov.au/internet/main/Publishing.nsf/Content/health-npaac-publication.htm
[NPAAC2007]	National Pathology Accreditation Advisory Council, 2007, Requirements for Information Communication (2007 Edition), ISBN: 1-74186-343-0	NPAAC 2006	http://www.health.gov.au/internet/main/Publishing.nsf/Content/health-npaac-docs-gudatco.htm
[NPMF2008]	NEHTA's Privacy Management Framework	NEHTA 2008	Reference in preparation for future release.
[OLDP2006]	Australian Government, January 2006, Health Insurance Act 1973, Office of Legislative Drafting and Publishing (OLDP),	NPAAC 2006	http://www.comlaw.gov.au/comlaw/Legislation/ActCompilation1.nsf/0/EF9FC45D70EA7B2FCA2570F2007D23A8?OpenDocument
[RCPA2004]	Royal College of Pathologists of Australasia, November 2004, Chain of Information Custody for the Pathology Request-Test-Report Cycle in Australia, RCPA.	RCPA 2004	
[RCPA2007]	The Royal College of Pathologists of Australia, Guideline, Australian Privacy Principles (13 March 2007).	RCPA 2007	
[PATH-PRR-SDT]	Pathology Result Reporting Package v1.0 – Structured Document Template v0.4	NEHTA 2008	http://www.nehta.gov.au/ (Home > Publications)
[UML4ODP_FDIS]	Final Draft International Standards, use of UML for ODP system specifications		
[UMLRMV2]	The Unified Modelling Language Reference Manual, Second Edition.		

Related Reading

The documents listed below may provide further information about the issues discussed in this document.

Related Documents			
[REF]	Document Name	Publisher	Link
[AAPP2000]	AAPP, June 2000, Review of Commonwealth Legislation regarding Pathology,	AAPP 2000	
[AAPP2002]	AAPP, January 2002, Privacy Policy in Community Pathology, Revision 1.2, AAPP	AAPP 2002	http://www.aapp.asn.au/Library/PrivacyPolicy.pdf
[AMA2002]	Australian Medical Association, 2002, AMA Position Statement Patient Follow-up and Tracking, AMA	AMA 2002	http://www.ama.com.au/web.nsf/doc/SHED-5HY37P/\$file/healths_gd_ps_pat%20foll%20up%20&%20track.pdf
[NEHTAWEB]	NEHTA Web Site	NEHTA 2008	http://www.nehta.gov.au/ (Home > Publications)