1. Statement

Queensland Health is increasingly using digital capabilities to improve patient safety and service quality, and efficiency through the health system. The sector is also seeing increasing digital disruption through the Internet of things and a convergence between what was traditionally biomedical and more conventional technologies. Patient involvement is also increasingly occurring via digital mediums with increased demand for appropriate access to data for secondary use.

Queensland Health’s Enterprise Architecture provides a way to ensure that current and future business, information and technical changes support the Department’s vision, strategic plans, and performance objectives, while meeting individual objectives.

The Queensland Health Enterprise Architecture extends the Queensland Government Enterprise Architecture to categorise specific Departmental content.

The Queensland Health Enterprise Architecture guides decision making by identifying applicable policies and standards aligned to five architecture domains with a framework (business, information, application, technology and information security).

2. Purpose

This policy reflects the changing nature of technology and its role in healthcare delivery and administration. Such a policy is essential in order to maintain the integrity of the Queensland Health information ecosystem in a time of increased local demand and rapid innovation to support patient centric integrated digitally enabled services. The intent of this policy is to ensure that:

- Information, Communications and Technology (ICT) enabled solutions and services are designed, implemented and managed according to the requirements of the Queensland Health Enterprise Architecture to ensure efficient and effective use, and management, of information and ICT solutions and services.
- The Department of Health provides quality ICT solutions and services which have been developed in a cost effective and cost-efficient manner.
- ICT solutions and services are positioned for growing demands and future needs of Queensland Health.
- Interoperability between ICT solutions and services enables secure exchange of trustworthy information across the continuum of care.

3. Scope

This policy applies to all employees, contractors and consultants within the Department of Health Divisions and Commercialised Business Units (CBU).

Compliance with this policy is compulsory.

4. Principles

- **Patient centricity.** Patients do not distinguish between care settings, organisational or jurisdictional boundaries. To the extent permitted by law neither should Queensland Health. All architectures, digital capabilities and underpinning technologies must therefore:
  - Allow patients to be better connected and engaged in their care.
- Support a patient's longitudinal record being able to be accessed, viewed, updated, and shared wherever the patient is located (i.e. regardless of care setting, organisation or specific application that may contain their information).

- Consider the needs of the health system not just a specific business or clinical need: The digital health ecosystem is a complex set of integrated services, applications and technologies. Given the dependence on technology for business continuity, the impact of implementing new or changed solutions or decommissioning existing solutions must be assessed and tested to a level commensurate with Queensland Health’s risk appetite.

**Queensland Health is federated.** Multiple care providers and care settings mean the architecture, and any specific digital investments must focus not just on individual needs, but also on the collaboration between providers and organisations. This is to be achieved by appropriate solution design, information sharing, architectural, investment and information governance and the interoperability of health systems and technologies.

**Sharing of information is essential, and collaboration on technologies is encouraged.** Division’s shall leverage common technology to support common functions and must not jeopardise the performance of the health system as a whole. Divisions and CBUs shall look to leverage existing investment to minimise cost and complexity where possible.

**Information as a health system asset.** This principle recognises the need to share information appropriately, increase access, manage its quality and subject it to appropriate governance, and lifecycle management processes. Interconnected organisations and intelligent enterprises need access to data for enhanced delivery. Timely and accurate information regardless of source is also essential for population health management, integrated care, and for appropriate secondary use.

**Managing technology diversity.** Collaboration is actively encouraged to minimise the diversity of solutions. This balances the need for best of breed solutions for a particular clinical or corporate practice with the need to minimise complex integration and the cost of having multiple technologies all of which need to be managed. ICT-as-a-service and/or cloud offerings should also be considered as an alternative to purchasing assets or maintaining systems in-house.

**Pragmatic and co-designed.** Architectures both at the enterprise and solution level are sustainable, with clear recognition of what today's business and technology environment looks like, whilst keeping abreast of emergent and future trends. Investments should be built such that the ICT environment can quickly respond to changes in health delivery needs and/or can cope with advances in technology. Solutions should be proposed and co-designed using appropriate stakeholder engagement and participatory governance.

**Appropriate sourcing and sharing of data.** Solutions should recognise, and use correctly, with appropriate curated duplication, the authorised data and/or functionality within the appropriate context. Departmental representatives shall avoid creating duplicate sources and/or repositories of data.

**Privacy, Confidentiality and Security.** The increased ability to share data in a more connected, digital world will be balanced by (authorised and appropriate) measures to restrict access to, and use of, patient information. Subject to these limitations Queensland Health will to the extent possible share information and enable big data.
5. **Requirements**

### 5.1 Enterprise Architecture

5.1.1 Decisions on the use of and investment in ICT shall align with the Queensland Health Enterprise Architecture.

5.1.2 The Queensland Health Enterprise Architecture shall align with and extend the Queensland Government Enterprise Architecture.

5.1.3 The Queensland Health Enterprise Architecture shall include five enterprise architecture domains to assist with organisation, navigation and understanding of what is relevant, applicable and useful. The five domains are business, information, application, technology, and information security.

5.1.4 Compliance with the Queensland Health Enterprise Architecture shall require compliance with all elements of the architecture.

### 5.2 Enterprise Architecture compliance and Dispensations

5.2.1 All digital solutions are subject to the requirements of the eHealth Investment Governance Framework.

5.2.2 Divisions and CBUs shall ensure that use of and investment in ICT and Information Management are aligned to the Queensland Health Enterprise Architecture.

5.2.3 Divisions and CBUs shall comply with the published mandated architectural standards, roadmaps and supporting artefacts.

5.2.4 To assist with whole-of-government compliance, Divisions and CBUs shall conduct a self-assessment against this Policy and submit their compliance statement to Queensland Health's Chief Information Officer by the end of each financial year.

5.2.5 Divisions and CBUs will provide, on request, accurate and comprehensive information to Queensland Health's Chief Information Officer, in order for Queensland Health to meet the mandated reporting requirements defined in the Queensland Government Enterprise Architecture Information Standard 2 (ICT Resources Strategic Planning). This includes at-risk system reporting, unsupported technology reporting and the annual current state ICT Profile report.

5.2.6 A formalised dispensation process shall be established to enable flexibility in meeting the variations and demands of the Department of Health.

5.2.7 To request a dispensation, an organisational unit shall undertake its own risk assessment; provide details regarding the impact of non-compliance, remedial action to be undertaken, associated costs and benefits of non-compliance and agreement to a timeframe to achieve compliance.

5.2.8 To seek a dispensation to this policy, Divisions and CBUs shall submit a request and rationale to the Design Authority for consideration and where necessary referred to the Architecture Standards Committee. Refer to the Enterprise Architecture Dispensation Standard for additional information.

5.2.9 For dispensations in relation to information management Divisions and CBUs shall submit a request and rationale to the Information Management Strategic Governance Committee (IMSGC).

**Note:** Refer to Appendix 1 Queensland Health Enterprise Architecture Committee Governance pathways for roles and responsibilities of relevant governing bodies.
5.3 Enterprise Architecture Domains

5.3.1 Queensland Health’s Chief Information Officer shall ensure that architectural standards and supporting guidance are published and maintained to ensure architectural needs are clear, structured around the five domains (business, information, application, technology, and information security).

5.3.2 The business architecture shall be the starting point for ICT planning and execution by describing the Department’s mission and how the means (capabilities, services, processes, functions) that is critical to achieving this mission are organised and executed.

5.3.3 Information resources shall be planned and managed in accordance with the Information Architecture and the Queensland Health Information management principles to ensure that information is trustworthy and appropriately available for use throughout Queensland Health.

5.3.4 The Department’s application portfolio shall be planned and managed in accordance with the application architecture to ensure a flexible, integrated, and reusable portfolio of applications that are effectively configured to meet the needs of the organisation and its stakeholders.

5.3.5 The technology portfolio shall be planned and managed in accordance with the technology architecture to ensure the integrity, availability and reuse of the technology capabilities required to support the application portfolio and information portfolio.

5.3.6 The Department of Health’s information resources, application and ICT portfolios shall be protected in accordance with the Information Security Policy Framework to ensure that new methods for delivering services are secure, in balance with maximising user convenience and productivity.

Note: The information security architecture that is described in the Information Security Standard is based on the following goals of information security:

- Confidentiality: ensuring that information is accessible only to those authorised to have access
- Integrity: safeguarding the accuracy and completeness of information and processing methods
- Availability: ensuring that authorised users have access to information and associated assets when required.

Information and the supporting processes, systems and networks are important business assets. Confidentiality, integrity and availability of information may be essential to maintain competitive edge, cash-flow, profitability, legal compliance and commercial image.

Refer to the Information Security Policy Framework for further information.

6. Legislation

- Electronic Transactions Act 2001
- Financial Accountability Act 2009
- Financial Accountability Regulation 2009
- Financial and Performance Management Standard 2009
- Hospital and Health Boards Act 2011
- Information Privacy Act 2009
- Public Health Act 2005
- Public Interest Disclosure Act 2010
7. Whole of Government

Department of Science, Information Technology and Innovation (DSITI):
- Queensland Government Enterprise Architecture Framework 2.0 (QGEA)
- Queensland Government Application Classification Framework
- Queensland Government Application Portfolio Framework Detail
- Queensland Government Business Process Classification Framework
- Queensland Government Enterprise Architecture Framework 2.0 (QGEA)
- Queensland Government Information Classification Framework
- Queensland Government Information Principles
- Queensland Government Information Security Classification Framework
- Queensland Government Information Security Policy Framework
- Queensland Government Technology Classification Framework

8. Supporting documents

Queensland Health Enterprise Architecture Framework
Department of Health:
- Digital Portfolio Governance Policy
- Information Security Policy
- Recordkeeping Policy
- Risk Management Policy

9. Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>A software system deployed by the agency which has part of an agency's business process embedded with it, for example, SAP.</td>
</tr>
<tr>
<td>Artefact</td>
<td>Artefacts are documents that are components of the Queensland Health Enterprise Architecture Framework including but not limited to the policy, architectural standards, protocols, procedures, positions and guidelines.</td>
</tr>
<tr>
<td>Common</td>
<td>Services and ICT that support health service delivery activities across some Hospital and Health Services or in use by more than one Division. Common is one of the three categories in the applications portfolio with Core and Local.</td>
</tr>
<tr>
<td>Core</td>
<td>Services and ICT that support health service delivery activities that are performed state-wide. Core is one of the three categories in the applications portfolio with Common and Local.</td>
</tr>
<tr>
<td>Dispensation</td>
<td>For the purpose of this policy, the term ‘dispensation’ means the endorsed exception from compliance with the enterprise architecture.</td>
</tr>
<tr>
<td>Enterprise</td>
<td>The Department of Health and the Hospital and Health Services (HHSs) make up the public healthcare system known as Queensland Health. The use of the word enterprise within this document indicates the public healthcare system as it is influenced by enterprise architecture.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enterprise Architecture</td>
<td>The practice of applying a comprehensive and rigorous method for describing a current and future structure and behaviour for an organisation's processes, information, applications, technology and human resources, so that they align with the organisation's strategic direction.</td>
</tr>
<tr>
<td>Enterprise ICT Service</td>
<td>Enterprise ICT Services are described in the ICT Service Catalogue available on the QHEPS intranet.</td>
</tr>
<tr>
<td>Fit for purpose</td>
<td>The extent to which the current functionality of the Information Asset/Application/Technology meets the need of the particular business area (NB: not the entire business of the agency) in which it is used.</td>
</tr>
<tr>
<td>Information Model</td>
<td>The Queensland Health Information Model refers to the collection of models, data set specifications (DSS) and standards that have been iteratively developed across the organisation. Key sources of data standards include the Queensland Health Data Dictionary and the Corporate Reference Data System. Within the department, the information model equates to an enterprise information model.</td>
</tr>
<tr>
<td>Internet of things</td>
<td>The Internet of things is the network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators, and connectivity which enables these objects to connect and exchange data.</td>
</tr>
<tr>
<td>Local</td>
<td>Services and ICT that support activities that may be specific to a local area or that arise from local innovation (e.g. only application to one team, unit or HHS). Local is one of the three categories in the applications portfolio with Core and Common.</td>
</tr>
<tr>
<td>Principles</td>
<td>Principles represent the Information and Communication Technology (ICT) interpretation and application of the organisation's mission and philosophy. They are fundamental and apply to all levels of ICT initiatives from EA to specific solution implementations. Adherence to the principles ensures alignment to organisational strategy and intent and results in a sustainable ICT environment.</td>
</tr>
<tr>
<td>Mandated/ Mandated Options</td>
<td>If an applicable position states a mandated product/service, it must be used. If there are multiple products/services for an applicable position, one of products/services must be used. A dispensation is required to not use a mandated product/service.</td>
</tr>
<tr>
<td>Preferred</td>
<td>If an applicable position states a preferred product/service it should be the first option considered and the full implications should be carefully evaluated before implementing an alternate product/service.</td>
</tr>
</tbody>
</table>
## Version Control

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>05/06/2014</td>
<td>Effective date. New policy developed from Queensland Health Enterprise Architecture Framework.</td>
</tr>
<tr>
<td>1.1</td>
<td>10/06/2015</td>
<td>Transferred information to new template.</td>
</tr>
<tr>
<td>2.0</td>
<td>12/04/2018</td>
<td>Enterprise Architecture Framework Standard incorporated into the Enterprise Architecture Policy. Statement and Purpose has been reviewed and updated to reflect current business models. Principles reviewed to align with the current Enterprise Architecture Health Service Directive. Formal review undertaken. Approved ASC March 2018 Approved CE eHealth Queensland</td>
</tr>
</tbody>
</table>
## Appendix 1  Queensland Health Enterprise Architecture Committee Governance pathways

In accordance with the eHealth Investment Governance Framework, the Department’s Tier 3 Committee, the eHealth Executive Committee (eHEC) has delegated its authority for architectural matters as follows:

<table>
<thead>
<tr>
<th>Committee</th>
<th>Responsibility</th>
</tr>
</thead>
</table>
| Architecture and Standards Committee (ASC) | **Accountable for:**  
- Approving co-designed architecture and security strategies, ICT policies and standards, roadmaps and guidelines.  
- Approving architecture and security standards.  
- Approving Enterprise Architecture Dispensation requests for Queensland Health where:  
  - the total investment value is >$500,000 or  
  - impacts more than one HHS or  
  - are high risk or high complexity.  
- Reviewing and endorsing all Queensland Health Architectures including segment and program architectures. |
| Information Management Strategic Governance Committee (IMSGC) | **Accountable for:**  
- Approving the enterprise wide data model, data definitions, reference data sets, terminology and data supply requirements (i.e. collections) developed for Queensland Health following endorsement from the relevant IMSGC working group.  
- Approval of information management strategies, roadmaps, policy, standards and guidelines that enable the safe, efficient and effective healthcare  
- Approval of strategic information management initiatives.  
- Approving information management practices and associated material.  
- Approving Information Management dispensation requests for Queensland Health.  
- Approving appropriate definition, publication and alignment of key state-wide information management deliverables such as an enterprise data dictionary, enterprise data model and requirements.  
- Approving the appointment of Data and Application custodians.  
**Exclusions:**  
The decision-making rights of the IMSGC exclude where:  
- It meets the criteria for ASC consideration (e.g. security policy, architectural standards, strategic documents etc.).  
- HHS information management for their own purposes.  
- Management of information is consistent with approved polices, standards and guidelines. |
| Information Security Committee (ISC) | **Accountable for:**  
Endorsing security strategies, polices and standards, roadmaps and guidelines. |
<table>
<thead>
<tr>
<th><strong>Design Authority (DA)</strong></th>
<th><strong>Accountable for:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Approving, rejecting or requesting changes to digital health initiative architectures at various stages in the solution’s lifecycle.</td>
</tr>
<tr>
<td></td>
<td>The authority of the DA includes solution architectures where:</td>
</tr>
<tr>
<td></td>
<td>• the initiative impacts more than one HHS and/or</td>
</tr>
<tr>
<td></td>
<td>• the initiative requires the use of core or common systems or services.</td>
</tr>
</tbody>
</table>

**Exclusions**

The decision-making rights of the DA exclude solution architectures where:

- it meets the criteria for ASC consideration (refer to ASC for criteria)
- the initiative impacts one HHS (including data) only
- initiative does not require the use of core and/or common systems or services
- it is a business as usual solution change request (not significant change) or is for access to solution data only.

For more information on the roles and responsibilities of the committees refer to the individual Terms of Reference.