1. Statement
The Department of Health (the Department) is committed to adopting a consistent and appropriate approach to the use of electronic approvals to ensure compliance with applicable regulatory and legislative requirements.

2. Purpose
The purpose of the policy is to ensure consistent, authorised and lawful use of electronic approvals by ensuring:

- compliance with departmental and whole-of-government policies, and State and Federal legislation
- legal and technical implications are carefully assessed when considering the use of electronic approvals or implementing a technology solution for electronic approvals
- all departmental staff are informed of their obligations and accountabilities.

3. Scope
This policy applies to all employees, contractors and consultants within the Department of Health divisions and commercialised business units.

This policy may be adopted by Hospital and Health Services (HHS) and re-branded as a local HHS policy, or used as a base for a local HHS policy.

This policy does not:

- mandate the use of electronic approvals for individual instances
- in any way limit the right of the Department or a third party to conduct a transaction on paper
- apply to any situation where a written signature is required by law.

4. Principles
The Department has adopted the following principles with respect to the use of electronic approvals:

- **Authentication** – the authenticity of the person(s) involved with the transaction can be verified
- **Confidentiality and Privacy** – information shared in all electronic communications must comply with confidentiality and privacy laws
- **Consent** – both the person(s) approving the document, and the person(s) receiving the document, consent to using electronic approvals as a method of transaction
- **Data integrity** – electronic communication cannot be changed, either during transit or once the data is at rest, without detection
- **Non-repudiation** – person(s) involved with a transaction cannot deny their involvement in that transaction
- **Recordkeeping** – all electronic communications must comply with the Department’s legislative obligations under the *Public Records Act 2002* (Qld) [refer to the Department’s Recordkeeping Policy];
- **Reliability** – the method used for electronic approval is reliable and appropriate for that transaction
5. **Requirements**

As a minimum, the following is required regarding persons using electronic approvals:

- they must have been issued with required Queensland Government security photograph identification
- they must have a unique login – username and password, which must be kept and used in a secure manner as required by departmental policy, and not be shared or disclosed to others on any occasion.

Electronic approvals must be managed in accordance with the following requirements:

5.1 departmental delegations

5.2 the Department’s Recordkeeping Policy, and any other relevant departmental policy that may apply to the transaction

5.3 a risk assessment (using the Departments risk management framework) of the transactional processes to carefully consider legal and technical implications must be conducted and captured be undertaken by the appropriate delegate

5.4 Application Custodian must ensure the software system (an application) meets the requirements of the policy

5.5 All principles must be complied with.

6. **Legislation**

- Acts Interpretation Act 1954
- Electronic Transactions (Queensland) Act 2001
- Evidence Act 1977
- Financial Accountability Act 2009
- Financial and Performance Management Standard 2009
- Hospital and Health Boards Act 2011
- Information Privacy Act 2009
- Public Records Act 2002

7. **Supporting documents**

**Queensland Government**

- Queensland Government Chief Information Office, Use of Electronic Signature
- Code of Conduct for the Queensland Public Service
- General Retention and Disposal Schedule for Administrative Records
- Information Standard 18: Information Security (IS18)
- Information Standard 31: Retention and disposal of public records
- Information Standard 34: Metadata
- Information standard 40: Recordkeeping
- Queensland Government Information Security Classification Framework (QGISCF)
- Queensland Government Information Security Controls Standard (QGISCS)

**Department of Health**

- Electronic Approval Guideline
- Electronic Approval Impact Assessment Checklist
8. Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved electronic approval method</td>
<td>An approved method in accordance with applicable state and federal laws, and which specifies the form of the electronic approval, the systems and procedures used with the electronic approval, and the significance of the use of the electronic approval.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Process that verifies the claimed identity of an individual as established by an identification process. Note: Authentication is the process used to verify the identity of a staff member providing an electronic approval.</td>
</tr>
<tr>
<td>Certificate</td>
<td>An electronic document used to identify an individual, server, a company, or some other entity and to associate that identity with a public key. A certificate provides generally recognised proof of an entity's identity.</td>
</tr>
</tbody>
</table>
| Confidentiality and Privacy | Ensuring that information is accessible only to those authorised for the relevant transaction and is protected from unauthorised disclosure or intelligible interception. In addition, any information shared in electronic communication must comply with confidentiality and privacy laws. **Confidential Information means:**  
  - any information which by its nature is confidential, is received on the understanding that it is confidential, or is marked as being confidential; and  
  - ‘confidential information’ as defined in s.139 of the *Hospital and Health Boards Act 2011*, namely, information that may identify a person (living or deceased) who has, at any time, received a public sector health service. **Personal Information:** has the same meaning as in s.12 of the *Information Privacy Act 2009*, namely, information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. |
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consent</td>
<td>Consent includes consent that can reasonably be inferred from the conduct of the person concerned, but does not include consent given subject to conditions unless the conditions are complied with.</td>
</tr>
<tr>
<td>Cryptography</td>
<td>Cryptography embodies principle, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or its unauthorized use.</td>
</tr>
<tr>
<td>Data</td>
<td>The representation of facts, concepts or instructions in a formalised (consistent and agreed) manner suitable for communication, interpretation or processing by human or automatic means. Typically comprised of numbers, words or images. The format and presentation of data may vary with the context in which it is used. Data is not information until it is utilised in a particular context for a particular purpose. Examples include; coordinates of a particular survey point; drivers licence number; population of Queensland; official picture of a Minister in jpeg format.</td>
</tr>
<tr>
<td>Digital signatures</td>
<td>Digital signatures which uses encryption and decryption technology alongside a Public Key Infrastructure (PKI). Data appended to, or a cryptographic transformation (see cryptography) of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient. Not just a digitised image of someone’s signature.</td>
</tr>
</tbody>
</table>
| Document(s)                               | Schedule 1 of the Acts Interpretation Act 1954 (Qld), defines a ‘document’ as:  
   (a) any paper or other material on which there is writing; and  
   (b) any paper or other material on which there are marks, figures, symbols or perforations having a meaning for a person qualified to interpret them; and  
   (c) any disc, tape or other article or any material from which sounds, images, writings or messages are capable of being produced or reproduced (with or without the aid of another article or device). |
| Electronic                                | Electronic relates to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.                                                                             |
| Electronic approval                       | The approval and/or signing process using an electronic signature that occurs online enabling individuals to authorise, sign and approve documents and transactions.                                                 |
| Electronic communication                   | Electronic communication means:  
   (a) a communication of information in the form of data, text or images by guided or unguided electromagnetic energy; or  
   (b) a communication of information in the form of sound by guided or unguided electromagnetic energy, if the sound is processed at its destination by an automated voice recognition system. |
<p>| Electronic document                       | Electronic document is any record created, communicated and maintained by means of electronic equipment.                                                                                                  |
| Electronic Document and Records Management System (eDRMS) | An automated system designed to manage semi-structured or unstructured content including text, images, and video content. A subset of the documents managed in an eDRMS can be declared to be records. The eDRMS manages these records using a rigorous set of business rules, which are intended to preserve the context, authenticity and integrity of the records. |
| Electronic record                         | Any record created, communicated and maintained by means of electronic equipment.                                                                                                                           |</p>
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic Signature</td>
<td>An electronic sound, symbol, or process, attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the record. An electronic signature must be attributable (or traceable) to a person who has the intent and authority to sign the record with the use of adequate security and authentication measures that are contained in the method of capturing the electronic transaction (e.g. use of a personal identification number (PIN) or unique log-in username and password), and the recipient of the transaction must be able to permanently retain an electronic record of the transaction at the time of receipt. Examples can include a digitised image of a handwritten signature, a code or PIN, and a mouse click on an “I accept” or “I approve” button.</td>
</tr>
<tr>
<td>Electronic transaction</td>
<td>A transaction conducted or performed, in whole or in part, by electronic means or electronic records.</td>
</tr>
<tr>
<td>Non-repudiation</td>
<td>The assurance that someone cannot deny something. Typically, non-repudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.</td>
</tr>
<tr>
<td>Principles</td>
<td>Key statements or concepts that guide all actions/practices within the purpose of the policy.</td>
</tr>
<tr>
<td>Private Key</td>
<td>An encryption/decryption key known only to the party or parties that exchange messages. In traditional private key cryptography, a key is shared by the parties so that each can encrypt and decrypt messages.</td>
</tr>
<tr>
<td>Public Key</td>
<td>A value provided by some designated authority as a key that, combined with a private key derived from the public key, can be used to effectively encrypt messages and digital signatures.</td>
</tr>
<tr>
<td>Public Key Infrastructure (PKI)</td>
<td>A form of information encryption that uses certificates to prevent individuals from impersonating those who are authorised to electronically sign an electronic document.</td>
</tr>
</tbody>
</table>
| Record(s)                     | A record is recorded information in any form, including data in computer systems created or received and maintained by an organisation or person in the transaction of business or the conduct of affairs and kept as evidence of such activity. (Aust. Standard AS4390) Records are information objects that document business activities and transactions. To be regarded as evidence a record must be complete. **Record means:** recorded information created or received by an entity in the transaction of business or the conduct of affairs that provides evidence of the business or affairs and includes—  
  (a) anything on which there is writing; or  
  (b) anything on which there are marks, figures, symbols or perforations having a meaning for persons, including persons qualified to interpret them; or  
  (c) anything from which sounds, images or writings can be reproduced with or without the aid of anything else; or  
  (d) a map, plan, drawing or photograph. |
<p>| Scanned signature             | A digital copy of a signature (converted to an electronic image file) derived from an original hand-written version.                                                                                                                                  |</p>
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Transaction  | The smallest unit of business activity. Processes resulting from undertaking a piece of business or the relationship between or within Public Authorities, between people or between a Public Authority and a person are all transactions.  
**Transaction includes:**  
(a) any transaction in the nature of a contract, agreement or other arrangement; and  
(b) any statement, declaration, demand, notice or request, including an offer and the acceptance of an offer, that the parties are required to make or choose to make in connection with the formation or performance of a contract, agreement or other arrangement; and  
(c) any transaction of a non-commercial nature. |

**Version Control**

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>5 July 2017</td>
<td>Approved CE eHealth Queensland</td>
</tr>
</tbody>
</table>