**National Authentication Service for Health Public Key Infrastructure**

**Relying Party Agreement**

**Parties**

**Commonwealth of Australia** as represented by the Australian Government Department of Human Services (**Human Services**)

**Relying Party**, being a Relying Party within the meaning of a Human Services Health Sector PKI Certificate Policy and a Health Network Certificate Policy concerning the National Authentication Service for Health (**Relying Party**)

**Definitions and interpretation**

1. In this agreement:
2. unless otherwise indicated, capitalised expressions have the same meanings as apply in a Human Services Health Sector PKI Certificate Policy and Human Services Health Network Certificate Policy concerning the National Authentication Service for Health (**NASH**) under which the Certificate being relied on has been issued
3. **‘Certificate’** means a Certificate issued under a Human Services Health Sector PKI Certificate Policy and a Human Services Health Network Certificate Policy concerning the NASH, including a Certificate renewed automatically by Human Services
4. **‘Clinical’** means anything that relates to the examination, diagnosis or treatment of individual patients by healthcare providers who are duly qualified, registered, recognised or trusted as performing those actions
5. **‘My Health Record system’** means the My Health Record system under the *My Health Records Act 2012*
6. **‘HI Service’** means, for the purposes of this agreement, the healthcare identifiers service operated by the Chief Executive Medicare as the service operator under the *Healthcare Identifiers Act 2010*, and includes the administrative extensions to that service for the registration of Supporting Organisations by Human Services
7. **‘Intermediary’** means an information technology provider that is a Relying Party and a Subscriber, and is engaged by a healthcare provider organisation for sending and receiving secure messages
8. **‘NASH Directory’** means a directory on which Human Services or its outsourced service provider publishes Certificates concerning NASH
9. **‘OCSP Responder’** has the meaning provided in clause 2
10. **‘Subscriber’** means the person that is the subscriber to, and the subject of, a Certificate
11. **‘Subscriber Terms and Conditions’** has the meaning provided in clause 4, and
12. references to documents are to the versions that are current from time to time.

**Commencement and duration**

1. In consideration for the PKI facility provided by Human Services that enables the Relying Party to rely on Certificates, the Relying Party acknowledges the terms and conditions on which it may so rely on Certificates, and this agreement will bind the Relying Party when it first:
2. relies upon a Certificate
3. uses a Key attached to a Certificate
4. authenticates a digital signature using a Key attached to a Certificate, or
5. accesses the NASH Directory, Certificate Revocation List or the Online Certificate Status Protocol Responder (**OCSP Responder**).
6. This agreement will continue to bind the Relying Party if and for so long as it asserts any reliance upon a Certificate or digital signatures generated using Keys attached to a Certificate. If the Relying Party does not agree with the terms of this agreement it must not rely on a Certificate or a digital signature generated using a Key attached to a Certificate.

**Subscriber Terms and Conditions**

1. This agreement binds the Relying Party in addition to any terms and conditions that bind it as a Subscriber for a Certificate (**Subscriber Terms and Conditions**) and in addition to the applicable Certificate Policy.

**Authorised reliance**

1. A Certificate does not verify or represent that the Subscriber is a particular organisation or a particular individual. The meaning of a Certificate issued under a Human Services Health Sector PKI Certificate Policy is nothing more and nothing less than a statement expressed in a digital format of the fact that the Subscriber is recorded as being registered with the HI Service.
2. A Certificate does not represent or verify that:

* the Subscriber has a particular identity (i.e. is a particular organisation or individual)
* the Subscriber or any of its personnel have particular qualifications or registrations other than with the HI Service, or
* the Subscriber is registered with the My Health Record system.

The registration of a Subscriber's identity is a separate process undertaken only when a Subscriber first applies for a Certificate.

1. The Relying Party may only rely upon a Certificate or digital signature generated using a Key attached to a Certificate for purposes authorised or approved by Human Services and published at [servicesaustralia.gov.au](http://www.humanservices.gov.au), including as authorised by the Certificate Policy under which it was issued. Any other reliance is at the sole risk of the Relying Party. Without prejudice to the generality of that limitation, messaging between parties that is not authorised by the Certificate Policy is at the sole risk of those parties.
2. Without limiting clause 7, Relying Parties must not use a NASH PKI Certificate by itself, and must use means other than reliance on the NASH PKI, to determine whether they will rely on the content of an electronic message or communication (including any Clinical statement or representation).

**Responsibility to take precautionary steps**

1. The Relying Party must (either itself or if it is a healthcare provider organisation through its Intermediary, if any) before relying on a Certificate (including a reliance for encryption purposes) or a digital signature generated using a Key attached to a Certificate:
2. verify the validity of a Certificate (i.e. verify that the Certificate is current and has not been revoked, by checking the Certificate Revocation List or querying the OCSP Responder)
3. check that the Subject of the Certificate identifies sending parties of an electronic communication who have used their Certificate for digital signing
4. check that the Subject of the Certificate identifies receiving parties of an electronic communication who have had their Certificate used for digital encryption
5. check that the intended use of the Certificate and digital signatures generated using Keys attached to the Certificate are for purposes authorised by the Certificate Policy under which it was issued.
6. The Relying Party must act reasonably in all the relevant circumstances where relying on a Certificate or a digital signature generated using a Key attached to a Certificate, including taking reasonable precautionary steps to address risk to the Relying Party from this reliance. Without limiting this requirement, Human Services may choose to publish (and maintain) information about what it considers to be reasonable precautionary steps at [servicesaustralia.gov.au/pki](http://www.humanservices.gov.au/pki)
7. If the Relying Party does not comply with clauses 9 and 10, any reliance upon a Certificate or a digital signature generated using a Key attached to a Certificate is solely at its own risk.

**Acknowledgement regarding compromised keys**

1. The Relying Party acknowledges that if a Private Key is compromised or stolen the messages sent and received using it will not be reliable or secure. Human Services cannot verify whether at any particular moment in time a Private Key has been compromised or stolen. The Relying Party must promptly notify Human Services in the event that it suspects that there has been a compromise of the Subscriber’s Private Key.

**Proper and lawful use**

1. The Relying Party must not perform any improper or unlawful act in connection with its use of a Certificate. The Relying Party acknowledges that a Certificate does not create or vest any authorisation to perform any act in connection with it, except as expressly stated in the applicable Certificate Policy.

**No agency**

1. The Relying Party is not an agent or representative of the Certification Authority or Human Services.

**Exclusion of liability**

1. The Commonwealth of Australia is not liable for any unauthorised, improper, negligent or unlawful use by the Relying Party or any other party of a Certificate or Key attached to a Certificate. The exclusions of liability and limitations of liability provisions contained in the Subscriber Terms and Conditions, applicable Certificate Policy, Root Certification Authority Certificate Policy, Root Certification Authority Certificate Practice Statement or Organisation Certification Authority Certificate Practice Statement apply to this agreement as if set out in it, with such changes as may be necessary to give them full force and effect.

**Disclaimer and exclusion**

1. The Commonwealth of Australia does not represent or warrant that any particular information technology provider’s system (or component of their system) that is used in connection with Human Services Health Sector PKI is fit for purpose, nor does it warrant the standards of performance or product of such a system (or component of such a system) or the supplier of such a system.
2. The Commonwealth of Australia does not represent or warrant that the variable components of a Certificate that can be defined by a Subscriber (i.e. the certificate usage and organisation unit name) are correct if they are varied from the default value of 'general'. The Relying Party acknowledges that Human Services has not verified such variances to this information and as such any reliance upon that information is at the sole risk of the Relying Party.
3. The Commonwealth of Australia is not liable to the Relying Party for any damages, loss or liability incurred by the Relying Party in connection with any illness, personal injury or death arising from or in connection with the use or reliance by the Relying Party or any other person of a Certificate or Key attached to a Certificate for messaging purposes.

**Variations of Relying Party Agreement**

1. Human Services may change or add to this agreement at any time, by giving the Relying Party notice by mail or electronically. A message sent to the Relying Party's business email address (as held in Human Services records) is one way of giving the Relying Party notice electronically.
2. When the Relying Party performs any of the acts described in clause 2 after the Relying Party has been notified of a change or addition to this agreement, the Relying Party will be taken to have agreed to the change or addition. This agreement may not be otherwise changed orally or by conduct of the parties.

**Applicable law**

1. This agreement is to be construed in accordance with the laws in force from time to time in the Australian Capital Territory and the parties agree to submit to the courts having jurisdiction in the Australian Capital Territory.
2. The parties intend that this agreement be legally binding on them.