Practice Incentive Payment (PIP)

## Practice Incentive Program eHealth Incentive (ePIP)

# Requirement 2—Secure Messaging Capability

The practice must have a standards-compliant secure messaging capability to electronically transmit and receive clinical messages to and from other healthcare providers, use it where feasible, and have a written policy to encourage its use in the practice.

The Royal Australian College of General Practitioners (RACGP) has developed a range of draft policy templates for general practices to adapt to their individual practice needs when registering and complying with the requirements for the Practice Incentive Program eHealth Incentive (ePIP).

The policy templates cover:

* secure messaging capability
* data records and clinical coding terminologies
* electronic transfer of prescriptions
* participating in the My Health Record.

These policies are to be used as a guide and must be individualised to suit your organisation’s particular needs. The RACGP advises not to implement these policies without first considering the specific needs of your practice.

The policy templates have been developed with current knowledge as of April 2016. The RACGP recommends that these policies be reviewed regularly.

[insert practice name]  *Practice policy on secure messaging capability*

Current as of: [insert date of last revision]

Version No:

To ensure that our practice utilises standards-compliant secure messaging systems that have the capability to both securely send and transmit clinical messages to and from other healthcare providers.

**Background**

Secure electronic messaging significantly lessens the chance of clinical information being accessed and read by a non-healthcare recipient. While electronic transmission carries an inherent risk of inadvertent wider broadcast of information, it also offers the opportunity to protect information more efficiently through higher security standards.

**Practice procedure**

Our practice:

* sends and receives correspondence and reports to and from our clinical desktop system to other healthcare providers through the use of conformant secure messaging software. *(In order to meet the Practice Incentive Program eHealth Incentive (ePIP) requirements, your practices must ensure that your software systems are compliant. You can consult the* [eHealth Product Register](http://pip.nehta.gov.au/ehealth-product-register) *for compliant software)*
* supports all healthcare providers in our practice to actively use secure messaging software to send and receive patient documentation, where feasible
* adheres to the use of compliant software to ensure that message contents are encrypted for the entire transmission process using appropriate digital certificates
* has verified that the installed software for SMD has been configured in accordance with Commissioning Requirements
* does not support or condone the use of insecure electronic methods of transmission for communications containing identifiable clinical information
* encourages a sustained increase in the use of standards-compliant secure messaging systems
* can demonstrate that the product is interoperable with other standards-compliant products on the eHealth Product Register
* uses a National Authentication Service for Health (NASH) Public Key Infrastructure (PKI) organisation certificate
* provides practice-based education and skills-based training to all healthcare providers and staff to ensure compliance with the policy and competency in the use of the technology.

**Software requirements**

The secure messaging software used in the practice is:

(List Secure Messaging Software here)

**Staff responsibility**

It is the responsibility of all healthcare providers in our practice to send electronic health information using secure messaging systems as outlined in this policy.

It is the responsibility of all administrative staff to support the use of secure messaging by undertaking any administration tasks involved in the maintenance or use of secure messaging systems. When any problems arise with the secure messaging software within our practice, the appropriate secure messaging software vendor and/or the company providing IT support for the practice will be contacted to assist in resolving the problem in a timely manner.

**Related resources**

RACGP *Standards for general practices* *(4th edition)*

<http://www.racgp.org.au/your-practice/standards/standards4thedition/>

RACGP Secure communications in General Practice – Product Listhttp://www.racgp.org.au/download/Documents/e-health/secure-communications-in-general-practice-product-list.pdf

RACGP *Computer and information security standards (2nd edition)*

<http://www.racgp.org.au/your-practice/ehealth/protecting-information/ciss/>

PIP eHealth Product Register

[www.nehta.gov.au/pip](http://www.nehta.gov.au/pip)

Disclaimer

The template policy is intended for use as a guide of a general nature only and may or may not be relevant to particular practices or circumstances. The RACGP has used its best endeavours to ensure the template is adapted for general practice to address current and anticipated future privacy requirements. Persons adopting or implementing its procedures or recommendations should exercise their own independent skill or judgement, or seek appropriate professional advice. While the template is directed to general practice, it does not ensure compliance with any privacy laws, and cannot of itself guarantee discharge of the duty of care owed to patients. Accordingly, the RACGP disclaims all liability (including negligence) to any users of the information contained in this template for any loss or damage (consequential or otherwise), cost or expense incurred or arising by reason of reliance on the template in any manner.