RACGP

RACGP e-health unit

Policy template

Practice policy on the use of standards-compliant secure messaging

The Royal Australian College of General Practitioners

The Royal Australian College of General Practitioners 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 eHealth Practice Incentive Program (ePIP).

The policy templates cover:

- secure messaging delivery
- clinical coding terminologies
- electronic transfer of prescriptions.

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

The policy templates have been developed with current knowledge as of January 2013. The College recommends that these policies will need to be regularly reviewed as new information comes to light and with the planned release, in June 2013, of the RACGP *Computer and information security standards* (CISS) second edition and CISS workbook.

In relation to all other computer and information security issues, until the release of the second edition of CISS, practices are advised that the current edition of the CISS (2011) is still best practice in providing guidance in information and security protection.

Disclaimer

The information set out in this document is intended for use as a guide of a general nature only and may or may not be relevant to particular practices or circumstances. Nor is this document exhaustive of the subject matter. Persons adopting or implementing any procedures and/or recommendations contained in this document must exercise their own independent skill or judgement or seek appropriate professional advice relevant to their own particular circumstances when so doing. While the text is directed to health professionals possessing appropriate qualifications and skills in ascertaining and discharging their professional (including legal) duties, it is not to be regarded as clinical advice and compliance with any procedures and/or recommendations cannot of itself guarantee discharge of the duty of care owed to patients and others coming into contact with the health professional and the premises from which the health professional operates.

Accordingly The Royal Australian College of General Practitioners and its employees and agents shall have no liability (including without limitation liability by reason of negligence) to any users of the information contained in this document for any loss or damage (consequential or otherwise), cost or expense incurred or arising by reason of any person using or relying on the information contained in this document and whether caused by reason of any error, negligent act, omission or misrepresentation in the information.

Name of practice:

Practice policy on the use of standards-compliant secure messaging

Purpose
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.

Related standards
RACGP *Computer and information security standards* – Section 3.12 p. 57
Secure electronic communication is a broad term which includes secure messaging via the public Internet. Secure messaging is a generic term that applies to all clinical information transferred between healthcare providers, healthcare organisations, patients, and trusted third parties.

Background and rationale
Secure message delivery (SMD) is due for release as an Australian Standard for interconnected point-to-point clinical messaging between SMD compliant software products.

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 (refer PIP eHealth Product Register[1])
- 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
- 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 PIP eHealth Product Register[2]
- 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)

---

[1] PIP eHealth Product Register, National E-Health Transition Authority. Available at: https://epipregister.nehta.gov.au/ [accessed 11 January 2013].
[2] Ibid.

The NASH organisation digital certificate used in the practice is:

(Details of Certificate including RA number and expiry date)

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*, fourth edition
www.racgp.org.au/your-practice/standards/standardsforgeneralpractices/

RACGP *Computer and information security standards* (CISS) and workbook (2011)
www.racgp.org.au/your-practice/e-health/cis/ciss/

PIP eHealth Product Register
www.nehta.gov.au/pip