Digitally signed by
National E-Health
Transition Authority
Ltd
Date: 2012.11.22
12:29:34 +11'00'

Securing eHealth information

A guide for healthcare providers

Governments across Australia have committed to a national approach to electronic health (eHealth) that will enable a safer, higher quality, more equitable and sustainable health system for all Australians.

eHealth is set to improve the healthcare system by transforming the way information is used to plan, manage and deliver health services. It will achieve this by using technology to improve access, transmission and recording of health information. This includes the ability to securely transfer information such as referrals, discharge summaries, test orders and results and prescriptions quickly and safely between healthcare providers. In addition, the Australian Government's personally controlled electronic health (eHealth) record system will allow healthcare providers to securely access key health information from a patient's health records.

Healthcare providers understand the need for patient privacy and confidentiality, and already have many processes, policies and procedures in place. However with the rollout of eHealth initiatives, additional security controls may be needed. Implementing these controls increases the level of protection of health information for both patients and healthcare providers and helps prevent inappropriate access.

As a healthcare provider you also benefit in knowing that information can be trusted, and can have confidence that eHealth information exchanges are secure and safe.

Why is security important?

Healthcare information has the greatest value when it is:

- Accurate
- Up to date
- Accessible where and when it is needed.

Without an effective security framework in place, health information may become unreliable or compromised (for example if it is accessed by unauthorised third parties). This could lead to degradation in the value of the information, may also cause the information to be withdrawn, and not be accessible where and when required.

How is health information currently protected?

Health information is protected by specific privacy laws in Australia, including Commonwealth (Cth), State and Territory legislation

- The Privacy Act 1988 (Cth) is the key piece of legislation in Australia and regulates how organisations collect, use, disclose and secure personal information and provides individuals with rights of access and correction. All health service providers are expected to comply with the Privacy Act
- The Personally Controlled Electronic Health Records Act 2012 provides further assurance by setting out civil penalties for unauthorised use, collection, disclosure of information held in a patient's eHealth record
- In addition to legal obligations, professional and ethical codes and standards also apply to healthcare providers to protect individuals' health information

September 2012

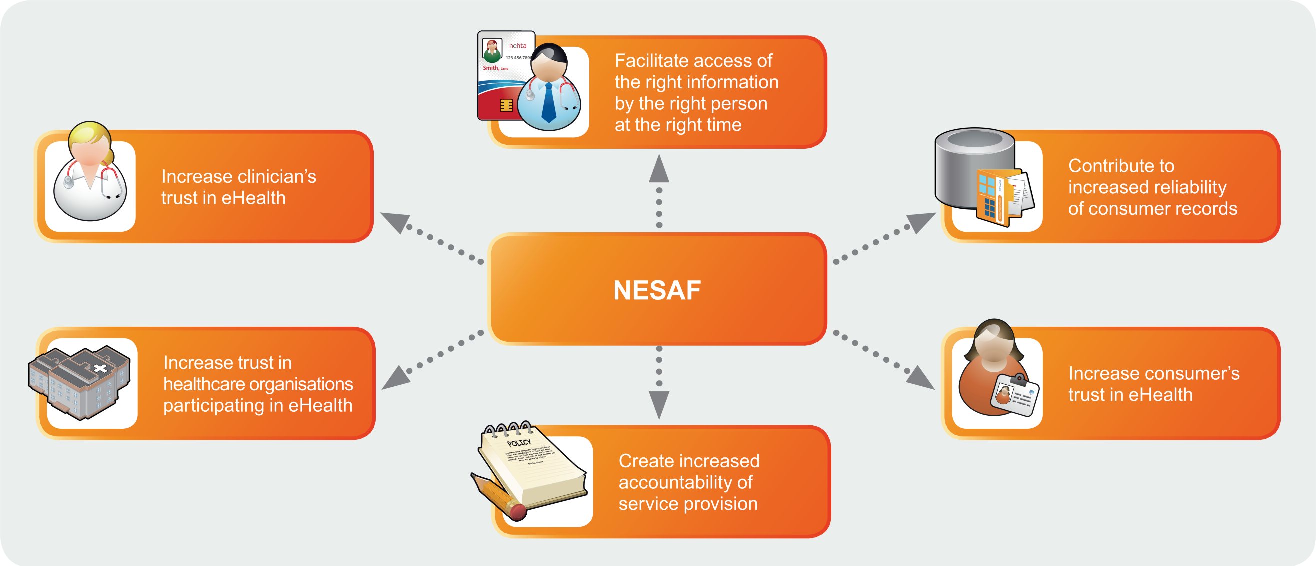
What is the National eHealth Security and Access Framework (NESAF)?

The National eHealth Security and Access Framework (NESAF) has been developed to provide the necessary security processes, tools, and information for you and your organisation to adjust to the new eHealth environment.

The NESAF:

- Will enable you to have confidence that health information contained in eHealth systems is secure, has not been tampered with or altered and is available to those authorised to have access when they need it
- Will help you and your healthcare organisation understand what is required to protect the confidentiality, integrity, and availability of healthcare information. It has been developed to underpin security and privacy in eHealth, and complements existing practices, controls and mechanisms
- Is a risk-based framework that can be tailored to organisations or practices of any size or complexity. It provides uniform guidance based on existing standards for healthcare and information security.

Benefits of the NESAF



NESAF

Facilitate access of the right information by the right person at the right time

Increase clinician's trust in eHealth

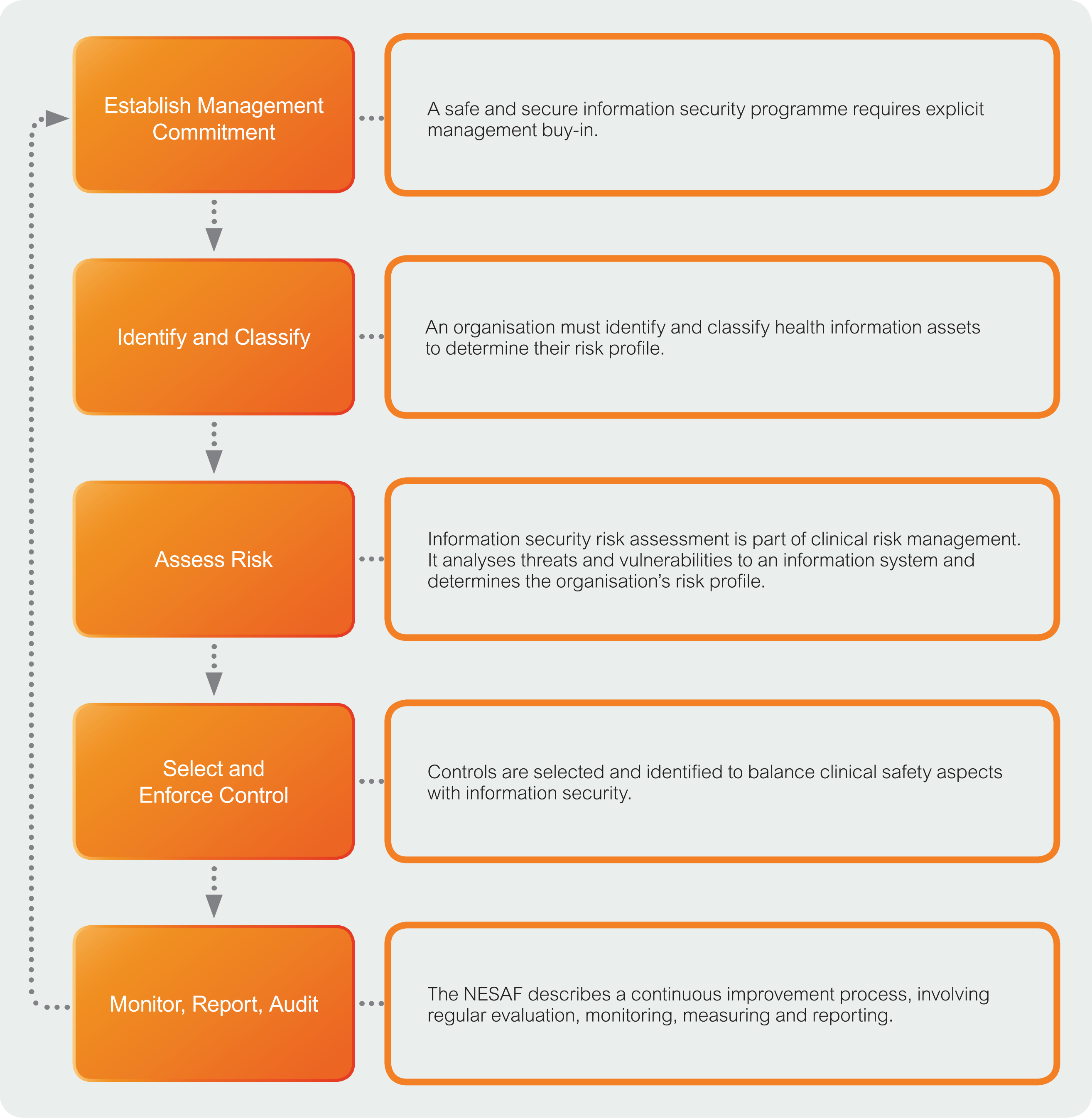
Contribute to increased reliability of consumer records

Increase trust in healthcare organisations participating in eHealth

Increase consumer's trust in eHealth

Create increased accountability of service provision

How does the NESAF work?
A risk-based approach



Establish Management Commitment

A safe and secure information security programme requires explicit management buy-in.

Identify and Classify

An organisation must identify and classify health information assets to determine their risk profile.

Assess Risk

Information security risk assessment is part of clinical risk management. It analyses threats and vulnerabilities to an information system and determines the organisation’s risk profile.

Select and Enforce Control

Controls are selected and identified to balance clinical safety aspects with information security.

Monitor, Report, Audit

The NESAF describes a continuous improvement process, involving regular evaluation, monitoring, measuring and reporting.

Who is responsible?

Information security is an integral aspect of clinical care, forming part of what is formally known as clinical risk management. Security of health information is everybody's responsibility, whether you are a healthcare provider, practice manager or administrative staff member.

People, processes and technology must all work together to ensure healthcare information systems are protected, safe and do not impede clinical workflow.

Different healthcare organisations will have different people responsible for information security.

If you have any questions about information security it is advisable to contact the staff responsible in your healthcare organisation.

The NESAF and the RACGP Computer and Information Security Standards (CISS)[1]

The RACGP has developed the CISS to work concurrently with the NESAF. The CISS adheres to the same goals of implementing safe security measures to protect patient information held and transmitted by electronic healthcare records

While the NESAF covers the whole of electronic infrastructure across the Australia's healthcare network, the CISS has been designed specifically for general practice. If Australian general practices comply with the CISS they can be confident that their security measures also comply with the higher level requirements of the NESAF.

nehta | eHealth

For more information on eHealth or the NESAF visit:
www.nehta.gov.au

[1] http://www.racgp.org.au/ehealth/ciss