Securing eHealth information

Is your business ready?

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 and patients to securely access key health information from a patient's health records.

Why is security important?

With the advent of eHealth, security is now more important than ever, as healthcare organisations increasingly use technology to facilitate patient healthcare, and to communicate between providers.

For any business in the healthcare system, robust security practices are required to both meet legal obligations and protect personal health information.

Greater collaboration and exchange of health information also creates an emerging set of business risks that need to be considered and addressed. All organisations involved in the provision of healthcare, whether they have many staff or are a sole practitioner, need to carefully manage the security of information systems and allow information to be available to the right person, at the right time and in the right form regardless of its origin, all the while supporting traceable provenance and control.

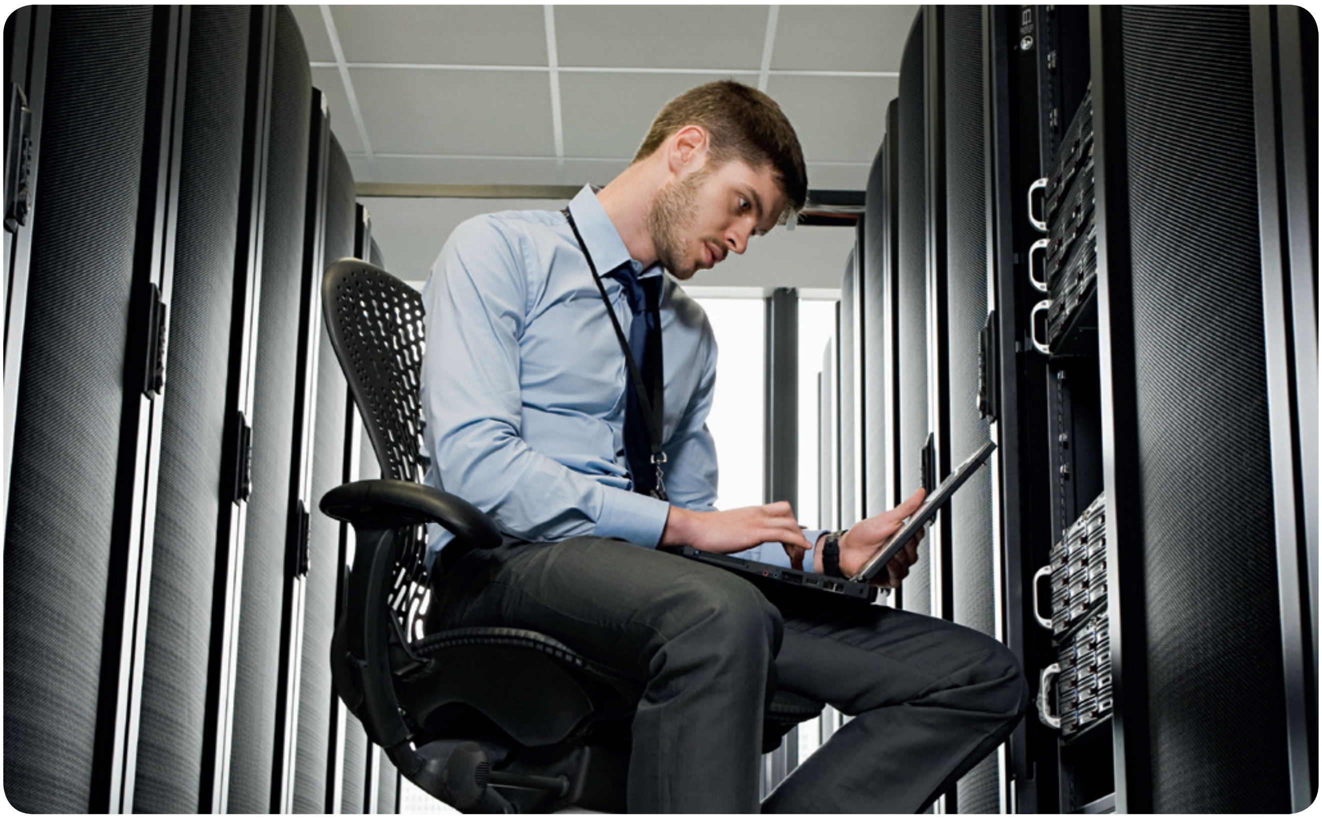
How is health information currently protected?

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 The Personally Controlled Electronic Health Records Act 2012 provides further assurance by setting out civil penalties for unauthorised use, collection and 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 your health information

September 2012

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

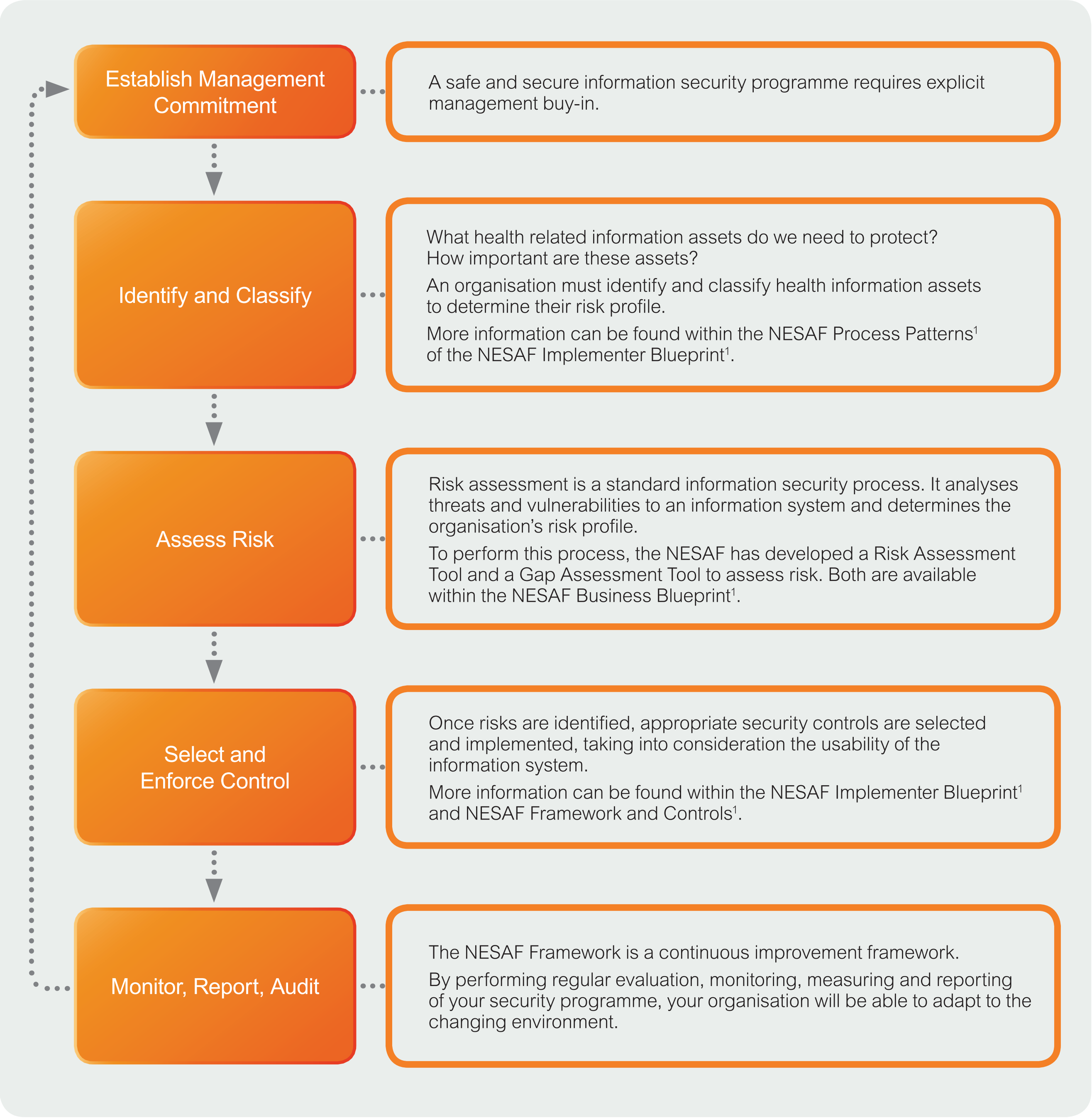


The National eHealth Security and Access Framework (NESAF) has been developed to provide you with the necessary security processes, tools and information for your business to adjust to the new eHealth environment. The NESAF is broader than any one implementation; it sets the language, concepts and expectations of security and access across Australia's healthcare system.

The NESAF:

- Aims to improve and complement existing processes, controls and mechanisms you may already have in place within your business, allowing you to participate securely in the emerging eHealth landscape
- Will help you understand your organisation's obligations to protect the confidentiality, integrity and availability of healthcare information, and how to meet those obligations
- Provides a risk-based approach, from risk identification and analysis to establishing appropriate security and access controls. The NESAF is scalable to different organisation types and sizes, as well as catering for varying complexity in information exchange. It provides uniform guidance based on existing standards for healthcare and information security.

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

What health related information assets do we need to protect? How important are these assets?

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

More information can be found within the NESAF Process Patterns[1] of the NESAF Implementer Blueprint[1].

Assess Risk

Risk assessment is a standard information security process. It analyses threats and vulnerabilities to an information system and determines the organisation's risk profile.

To perform this process, the NESAF has developed a Risk Assessment Tool and a Gap Assessment Tool to assess risk. Both are available within the NESAF Business Blueprint[1].

Select and Enforce Control

Once risks are identified, appropriate security controls are selected and implemented, taking into consideration the usability of the information system.

More information can be found within the NESAF Implementer Blueprint[1] and NESAF Framework and Controls[1].

Monitor, Report, Audit

The NESAF Framework is a continuous improvement framework.

By performing regular evaluation, monitoring, measuring and reporting of your security programme, your organisation will be able to adapt to the changing environment.

[1] Documents can be found at www.nehta.gov.au

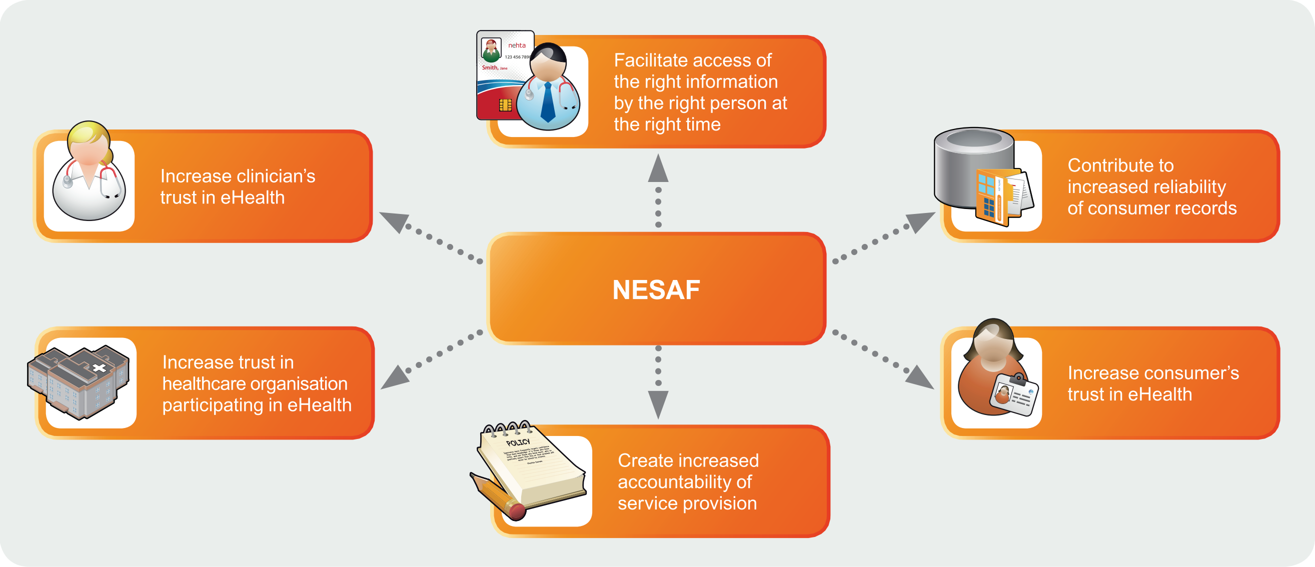
Why apply the NESAF?

The NESAF is broader than IT security as it involves people, process and policy.

The application of the NESAF will also help:

- Enhance your position of trust with patients and other providers in the eHealth space
- Promote confidence that health information contained within eHealth systems is secure, has not been tampered with or altered, and is available to those authorised to have access when they need it
- Reduce your vulnerability to information security threats
- Give you better control of the health information under your management
- improve your business processes and practice efficiency
- Allow you to better manage and monitor your risks
- Help you meet your legislative and policy obligations.

Benefits of the NESAF



NESAF

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

Contribute to increased reliability of consumer records

Increase consumer's trust in eHealth

Create increased accountability of service provision

Increase trust in healthcare organisation participating in eHealth

Increase clinician's trust in eHealth

nehta | eHealth

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