nehta

Level 25, 56 Pitt Street
Sydney NSW 2000
Telephone: (02) 8298 2600
Facsimile: (02) 8298 2666

8 February 2012

Mr James Catchpole
Committee Secretary
Joint Select Committee on Cyber-Safety
PO Box 6021
Parliament House
CANBERRA ACT 2600

Dear Mr Catchpole,

Thank you for the invitation to provide a submission to the Joint Select Committee on Cyber-Safety to assist its inquiry into cybersafety for senior Australians.

NEHTA is the lead organisation supporting the national vision for eHealth in Australia; working with consumers, healthcare providers, the ICT industry, and governments to enable safer, higher quality and sustainable healthcare. NEHTA is the managing agent for the development of the Personally Controlled Electronic Health Record (PCEHR) on behalf of the Department of Health and Ageing. Older Australians are one of the target groups in the community likely to receive the most immediate benefit from having a PCEHR.

This submission addresses the terms of reference of the Committee from the perspective of NEHTA's role in shaping eHealth technology in Australia, including the PCEHR Programme. Specially, this submission covers;

- NEHTA's understanding of cyber threats to older Australians relating to eHealth;
- How the PCEHR will benefit older Australians;
- How the PCEHR and other eHealth initiatives incorporate best practice cyber-safety safeguards.

1. Older Australians and Cybersecurity Risks

NEHTA recognises that older Australians are more likely than the average adult population to access health information via the internet[1], but they are however a more vulnerable group in terms of cybersafety, as they often do not have the years of experience that other members of the community have using computers and the internet as an integral part of everyday business.

While many older Australians are aware of the information available via the internet, they may also be more vulnerable to threats, and can be unaware of what may constitute risky online behaviour. Examples of this might include password strength and making robust choices about their sensitive information.

[1] Australian Communications and Media Authority, Use Of Digital Media And Communications By Senior Australians, 2009.p2.

NEHTA notes that older Australians may need additional, targeted measures and education to reduce risks to these threats.

NEHTA understands that older Australians:

- May have increased levels of trust, so are more vulnerable to social engineering [2]opportunities, and targeted phishing and SPAM emails;
- May have less developed computer skills and risk awareness, which makes them less likely to understand the need for protection against malware and antivirus;
- Are increasingly using the internet to seek health information.

2. Older Australians and eHealth

The increasing use of eHealth technology is occurring at the same time as our population is ageing and a corresponding increased burden on health services. eHealth has the potential to ease pressured on health services by making the safe and secure access to and communication of health information easier.

The Personally Controlled Electronic Health Record (PCEHR) System is the next step in using eHealth to enhance the healthcare system. The PCEHR System enables the secure sharing of health information between an individual's healthcare providers, while enabling the individual to control who can access their PCEHR.

Older Australians are a key target group for the PCEHR. The benefits of participation for this community are centred around improved continuity of care (thereby enabling improved management of chronic disease), improved coordination and follow-up post of acute episodes, reduced adverse drug events, and improved personal control over health information. In order for older Australians to fully benefit from the PCEHR it must be safe and easy to use. NEHTA does not regard it as acceptable to respond to cyber risks by limiting older Australians' access to online information and services, but will rather ensure that the PCEHR System is useable for those who stand to benefit from it the most.

The PCEHR Consumer Portal

Consumers may register for a PCEHR from July 2012. As part of registration, consumers many may choose to establish an online portal account for their PCEHR.

Older Australians' online interactions with the PCEHR will be via the consumer portal.

The consumer portal has the following functions:

- Verification of identity (validating the consumer is who they claim to be);
- Registration for PCEHR (allowing an individual to participate in the service by creating an active record);
- Nomination of representatives (such as relatives or other carers);
- Setting of access controls for providers (determining which providers may access their health information);
- Provision of educational material (including security and privacy awareness).

A range of functionality for PCEHR has been developed to specifically address the needs of older Australians.

- Legally authorised representatives (such as an enduring power of attorney) may register and control a PCEHR on their behalf, including via the online portal.

[2] Social Engineering is where individuals will be deceptively targeted with the intent of gaining confidential information, or undertaking actions, from them for someone else's gain. For example, an Older Australian being asked for their PIN Code from someone pretending to be from the Bank.

- Consumers' may nominate others with caring responsibilities (such as adult children) to access and assist in management of their PCEHR via the online portal.
- Assisted registration channels, including DHS Medicare offices and aged care facilities.
- End user education, including security awareness for both older Australians and their representatives.

A number of strategies will be employed to simplify use and encourage participation. Educational collateral will be developed which is specific to older Australians. This will include basic fact sheets, online tutorials; call centre support and shopfront access at Medicare offices. The PCEHR web Learning Centre will include resource packs for older Australians, including tailored information for carers. 'How to register' guides for consumers will also be made available. There will also be an assisted registration channel for older Australians who don't have internet access at home.

Information about eHealth reform, technologies and the PCEHR are available at www.yourhealth.gov.au.

3. Best Practice Safeguards implemented in eHealth

In the design and development of eHealth systems, NEHTA is implementing numerous controls to safeguard both the services, and those who will be using them.

NEHTA recognises and seeks to uphold the objectives of the Commonwealth Government Cyber Security Strategy[3].

- All Australians are aware of cyber risks, secure their computers and take steps to protect their identities, privacy and finances online.
- Australian businesses operate secure and resilient information and communications technologies to protect the integrity of their own operations and the identity and privacy of their customers.
- The Australian Government ensures its information and communications technologies are secure and resilient.

This third objective in particular is relevant to development and operation of eHealth in Australia and NEHTA has taken a comprehensive approach to meeting this objective.

A Multi-Layered Approach to Security

The PCEHR System utilises multiple layers of technical and non-technical controls in order to maintain security. These controls include authentication of authorised users, robust audit logs, proactive monitoring and reporting, rigorous security testing, governance and the provision of education and training materials to the users of the system.

In order to support the PCEHR, NEHTA has developed a range of foundational products which will provide key elements of privacy protection and security. Principal amongst these are the National Authentication Service for Health (NASH), and the National eHealth Security and Access Framework (NeSAF).

The National Authentication Service for Health (NASH)

The NASH addresses the need to ensure that eHealth transactions are private, traceable and only conducted by know entities. The NASH is Australia's first nationwide secure and

[3] Commonwealth of Australia 2010http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/%284CA02151F94FFB778ADAEC2E6EA8653D%29~AG+Cyber+Security+Strategy+-+for+website.pdf/$file/AG+Cyber+Security+Strategy+-+for+website.pdf

authenticated service for healthcare delivery organisations and personnel, and will be used to access the PCEHR and to exchange sensitive eHealth information. The service will issue digital credentials, including digital certificates managed through the Public Key Infrastructure and secured by tokens such as smartcards. These credentials will validate identity when used to access eHealth systems (including the PCEHR System) that are enabled to use NASH authentication.

The National eHealth Security and Access Framework

NEHTA has also developed the National eHealth Security and Access Framework (NeSAF), a set of tools designed to support organisations engaged in national eHealth. The NeSAF provides guidance to businesses in how to establish an information security infrastructure, for example by helping to assess security risks, and then selecting appropriate controls. It encourages businesses to adopt a consistent approach to the application of health information security standards, and provides better practice guidance in relation to eHealth-specific security and access practices. NEHTA has itself used the NeSAF in designing the PCEHR security architecture.

Building on Existing Security Frameworks

Core to the security development of the PCEHR is compliance to Commonwealth security standards, policies and frameworks, namely the Protective Services Policy Framework (PSPF), the Information Security Manual (ISM), and the National eAuthentication Framework (NeAF), in addition to alignment to the international best practice security management standards ISO/ECI27001. The security requirements for NEHTA's products are mapped to these frameworks. Additionally, NASH will be accredited to Gatekeeper, which is the Australian Government's strategy for the use of Public Key Infrastructure (PKI). NASH PKI Certificates will be used to authenticate both healthcare organisations and healthcare individuals.

Yours sincerely,

Peter Fleming
Chief Executive