Introduction
The Australian healthcare system is undergoing significant change in terms of collection, distribution and access to health information (Schaper & Pervan 2004). Australia is in the process of converting to an electronic health record (EHR) system with the National E-Health Transition Authority (NEHTA) identifying the need to accelerate the adoption of e-health (NEHTA 2009). Also, the Australian Federal Government has recommended that all healthcare professionals should adopt electronic information storage and exchange, eliminating the use of paper records, so as to enable a self-controlled EHR for every citizen, as well as improve the safety and quality of healthcare (Department of Health and Ageing 2009).

In September 2008, Northern Health was the first health service in the state of Victoria to implement a semi-electronic medical record (SMR). Northern Health sees this implementation as a step towards implementing an EHR. With the health industry moving towards the provision and use of electronic patient information, there is little, if any, published guidance around monitoring user access of electronic confidential health information.

Currently in Australia there is a system comprising a mix of paper and electronic systems. NEHTA states on its website that there are ‘no national security standards or accountabilities for access to systems in place. In the absence of a national scheme, health professionals and practices will increasingly adopt varying electronic means to store patient information – systems that may have limited interoperability and unverified security’ (NEHTA 2009).

While electronic systems enhance patient care, privacy and confidentiality concerns must also be considered. There are many examples of breaches of confidentiality in the public domain where health records have been viewed by those not involved in the patient’s care, and the subsequent reaction of the organisation to these events documented. What can organisations do to prevent unauthorised access? What systems should be in place as a preventive measure rather than a reactive action? This paper will discuss what security and monitoring measures could and should be taken to ensure that legitimate use of the SMR and eventually the EHR is occurring.

Background
As the world becomes more electronic, Northern Health is moving towards a digital environment. In 2008 Northern Health, in conjunction with its neighbouring mental health service, North Western Mental Health, implemented a scanned medical record, known as the Clinical Patient Folder or CPF. CPF has been implemented across 10 sites between the two health services and governed by two bodies. All patient information generated from 1 September 2008 is scanned into CPF and no longer maintained in hardcopy format as a paper-based medical record. CPF also has the functionality to allow users to complete electronic progress notes, which are completed by some clinicians in the Outpatient, Allied Health and Mental Health Divisions. Since the health service has gone live with CPF, over 370,000 electronic progress notes have been generated. Scanned documentation will continue to be archived in hard copy format until Northern Health complies with changes to legislation allowing destruction of digitised documentation (compliance expected in late 2011).

In Victoria, major metropolitan and regional health services are going down the path of implementing a scanned medical record system. A Scanning Special Interest Group has been established with Victorian and other Australian state health agencies, under the umbrella of the Health Information Management Association of Australia (HIMAA). The Special Interest Group is a structured forum that allows representatives from all health agencies across Australia to discuss common issues and experiences with a scanned medical record. The forum gives health agency representatives the opportunity to interact and provides a platform in contributing to relevant HIMAA state and national dialogue and strategy development.

Northern Health continues to work towards implementing an EHR that will interface with its scanned medical record. In order to facilitate this, more information technology infrastructure is required to allow clinicians to directly enter patient information in real time at the patient’s bedside. However, if Northern Health had a fully functional EHR today, how could we, as an organisation, ensure that the privacy and security of patient information is maintained in an electronic environment?

Australia’s health system in context
Healthcare in Australia is one of the country’s largest and most complex industry sectors, with a mixed system of...
federally-funded, state-managed and privately-owned healthcare provision. Currently, the healthcare system employs around 825,000 people (Australian Institute of Health and Welfare [AIHW] 2010). The population of Australia is 21.3 million; we have less than half the population of the UK and Italy (at 62 million and 60 million respectively) (AIHW 2010). Australia spends 9.1% of GDP on healthcare, Italy’s expenditure is 8.7% of GDP and the UK spends 8.4% on their healthcare system. Australia is ranked 8th among our OECD partners in terms of healthcare expenditure. The average Australian at birth age has a life expectancy of 81.4 years, which places Australia in the top 5 nations in the world (AIHW 2010).

**Drivers for e-health in Australia**

One in seven Australians now lives with a chronic or complex disease that can be challenging and expensive to treat. People living in rural and remote areas of Australia tend to have shorter lives and higher levels of illness and disease risk factors than those living in urban areas. Compared with major cities, remote areas have less than half the supply of medical practitioners and dentists (AIHW 2010). Telehealth has become established in Australia as a method of providing healthcare to patients who live in remote areas, or where access to healthcare services is inequitable.

It is noted that poor availability of health information across care settings can be frustrating and time consuming for patients and health professionals alike. Poor availability of patient information can also have damaging effects on a patient’s health outcomes through avoidable adverse drug events and lack of communication between healthcare providers. About 2 to 3% of hospital admissions in Australia are linked to medication errors, which equates to 150,000 admissions each year and costs the health system $660 million. About 8% of medical errors are because of inadequate patient information. Clear, quickly available information will reduce such incidents, avoid unnecessary tests and save scarce health resources. It is hoped that savings brought about by the introduction of e-health will allow funding to be targeted to these areas in need.

**e-Health in Australia**

A commitment was made in 1999 by the Australian Federal Government to move towards e-health, establishing the first e-health task force after recognising the benefits of an e-health strategy for safe patient care and for healthcare funding. In 2005, NEHTA was established to develop better ways of electronically collecting and securely exchanging health information.

The general practitioner (GP) sector in Australia has been using computers for clinical purposes for a long time. In 2006, 90% of GPs were using computers for clinical purposes, an increase from 15% in the mid 1990’s. More recently, the figure has been quoted at 98% of GPs, placing GPs at the forefront of electronic health in Australia (Royal Australian College of General Practitioners 2010). However, outside the GP sector, within hospital environments, progress has not been as far-reaching.

In all, there is a defined commitment by the Australian Government to pursue an electronic health record associated environment within Australia, with $466.7 million to be invested over the next two years with a defined need and want shared by both providers and consumers. However, limited progress has been made in tangible e-health systems actually in use so far, although there are pilot projects working, and pockets of development. Much work in Australia has been in standards development in security, design and a common language for exchange of information, rather than actual implementation of system thus far. This is partly due to lack of funds.

**Healthcare identifiers: the ‘spine’ to an e-health environment in Australia**

The ‘spine’ for an e-health environment is under implementation with the development of an individual healthcare identifier (IHI), and legislation passed in July 2010 paved the way for all Australians to be allocated an IHI. This identifier will form the spine for e-health infrastructure to enable the transfer of electronic health information across Australia between healthcare providers. This process is occurring nationally, to avoid system incompatibility between each state and to ensure secure electronic transfer of health information across the healthcare system. In all, three identifiers will be used: one for the individual, one to identify the healthcare provider and another to identify the healthcare organisation.

This initiative will facilitate information sharing between healthcare providers to support patient treatment and communication. Personally-controlled electronic health records will build on the foundation laid by the introduction of the IHIs from 2010 (Roxon 2010).

**A personally-controlled electronic healthcare record**

The national personally-controlled electronic healthcare record (PCEHR) system will be separate from the HI Service. The PCEHR will use identifiers to facilitate the identification of a consumer and healthcare provider. This will provide consumers and their healthcare providers with greater certainty that the individual’s information is being correctly attributed to their electronic record. Consistent with the National E-Health Strategy, endorsed by all Health Ministers, participation in a PCEHR will be voluntary and an individual’s IHI will only be used for their PCEHR with their permission.

Pilot sites in operation at present are located in New South Wales. In Victoria, a PCEHR is currently under development and pilot sites in Victoria that will link primary health service providers with hospitals will soon be underway. It is envisaged that within a PCEHR, patients will be empowered with easy-to-access information about their medical history, including medications,
test results and allergies, which will allow them to make informed choices about their healthcare. The personally-controlled electronic health record will have two key elements:

- a health summary view including conditions, medications, allergies, and vaccinations
- an indexed summary of specific healthcare events.

The National Health and Hospitals Reform Commission stated that:

by 2012, every Australian should be able to have a personal e-health record ... choose where and how their personal e-health record will be stored, backed-up and retrieved, and it should be … at all times owned and controlled by that person. (National Health and Hospitals Reform Commission 2009)

There will be much activity around PCEHR in the coming year.

Examples of e-health development in Australia

Two examples of e-health innovation in Australia are the Shared Electronic Health Record in the Northern Territory and Healthelink in New South Wales.

**The Shared Electronic Health Record**
The Shared Electronic Health Record is a summary of medical records that can be accessed by health professionals at the point of care. Information is transmitted for each visit to participating healthcare providers including public hospitals, health centres and GPs. The system records past and present treatments, current medications, test results and diagnoses, and focuses on Aboriginal health clients, who comprise about one third of the Territory's population and make up a considerable proportion of people who use health and community services. It is widely recognised that the health of Aboriginal and Torres Strait Islander people is generally much poorer than that of other Australians. Additionally most Aboriginal Territorians live in very remote communities and studies have identified that poor communication between sectors delivering health care to Indigenous people results in frequent readmissions, duplication of interventions, non-attendance of appointments due to frustrations with waiting times, and potential risk to the individual's health and wellbeing (NEHTA 2010).

**Healthelink**
Healthelink is an electronic health record piloted in NSW, which provides consumers, GPs, hospitals and community services in selected areas with an electronic healthcare record. Information collected includes diagnoses, medications, vaccination history, allergies, blood test results, and dates of contact with hospitals, GPs and community health centres. For example, a GP can view information related to recent hospital admissions as soon as the patient has left the hospital, rather than waiting days or weeks relying on conventional systems (NSW Health 2008).

These are two examples of e-health developments in Australia, which is an ongoing and evolving area. Australia is involved in the development of many standards relating to electronic health information. International standards on privacy and security of health information have been compiled and can be used by organisations when considering their move into an electronic health record environment.

**Privacy and IHI**
The combination of technology controls, specific controls set out in healthcare identifiers legislation, and existing privacy laws will provide strong privacy protections. There will be clearly established limits on the adoption, use and disclosure of healthcare identifiers. Healthcare identifiers can only be used for health information management and communication as part of the:

- provision of healthcare to an individual
- management, funding, monitoring or evaluation of healthcare
- provision of indemnity cover for a healthcare provider
- conducting research that has been approved by a Human Research Ethics Committee
- lessening or preventing a serious threat to an individual's life, health or safety or to public health or public safety.

The system design does not allow ‘browsing’ of records; a request by an authorised healthcare provider for a patient's identifier will only reveal an IHI when there is an exact match with patient information provided by the healthcare provider. Each time a record held by Medicare Australia is accessed, the details of by whom and when will be recorded in an audit log. Electronic communications involving healthcare identifiers will be made secure through the use of standardised public key infrastructure (PKI) and secure messaging services.

Legislation clearly sets out the permitted uses of healthcare identifiers. Penalties for the intentional misuse of healthcare identifiers, such as inappropriate disclosure of information by Medicare Australia or users of the service, will be set out in legislation. In addition, current privacy laws will continue to apply. The Federal Privacy Commissioner will monitor the operation of the HI service by Medicare Australia and handle complaints against the Commonwealth public sector and private sector organisations. Legislation relating to privacy in Australia exists both at a national and state level. Nationally, the Commonwealth Privacy Act regulates information held by government agencies and private organisations. In Victoria, health privacy is legislated under the Health Records Act and the Information Privacy Act. Like other privacy legislation in other countries, noncompliance with the Acts can result in penalties.

**Standards relevant to e-health records and security**

How, then, can a healthcare organisation attempt to ensure security of their e-health records? One way is to be guided by standards developed both locally (within
March 2011 | HIM-INTERCHANGE Vol 1 No 3 | ISSN 1838-8620 (PRINT) ISSN 1838-8639 (ONLINE) | 9

Australia) and internationally. Health organisations can ensure that relevant standards are incorporated into their systems when developing and purchasing e-health systems to assist in guarding the security of their health information. One such standard is IT014, an Australian standard currently under development. The standard will cover privacy of information, accuracy of data, availability of information, confidentiality of information, and integrity of data in relation to storage, use, transfer and retrieval of information. Included as part of the development of this standard is a rewrite of AS 2828 Medical Record Documents Standard, which is being upgraded to encompass electronic health information, including specific features to enable good transformation into an electronic format.

International Standard ISO 27799 provides guidance to healthcare organisations on how best to protect the confidentiality, integrity and availability of health information. The integrity of health information must be protected to ensure patient safety, and an important component of that protection is ensuring that the information’s entire lifecycle be fully auditable.

The need for effective IT security management in healthcare is made all the more urgent by the increasing use of wireless and Internet technologies in healthcare delivery. If not implemented properly, these complex technologies will increase the risks to the confidentiality, integrity and availability of health information.

What preventive measures can healthcare organisations put in place to minimise the threats to health information security? International Standards identify 11 security control clauses with minimum requirements in the protection of personal health information. Some examples of these controls include the following:

- an information security policy that provides a statement of direction and support for health information security
- human resources security with all employees security and privacy responsibilities outlined in their job descriptions.

Examples of communications and operations management security measures include:

- an audit trail for all new databases to audit actions performed within the database
- detection and prevention controls to protect against viruses
- encryption of information that is sent electronically between parties
- implementation of an organisational policy on electronic mail.

**Security controls in place at Northern Health**

Security controls are in place at Northern Health for our scanned medical record. With Northern Health being the first health service to go live with a scanned medical record in Victoria, a benchmark agency was identified and visited to seeking guidance on how to audit access to confidential electronic information. Following the benchmarking exercise, Northern Health has implemented four user access security audits in protecting patient privacy and security. These audits include:

- temporary access requests
- random staff access
- staff and/or hidden records access
- ad hoc requests/incidents (e.g. auditing the user access of a celebrity/public personality that has had contact with the health service).

To date, no major security breaches have been identified; however, vigilance and ongoing auditing continues.

Other security controls at Northern Health include the implementation of organisation-wide policies including:

- use of scanned medical record policy
- remote access to scanned medical record and other clinical systems policy
- privacy policy
- information technology security policy.

Northern Health continues to work with the vendors of all of our clinical and non-clinical information management systems in refining security controls in the protection of information.

**Conclusion**

This paper has discussed the emerging e-health environment in Australia, legislation that will support this development in Australia and the Australian healthcare environment. In conclusion, e-health is fast developing and the way in which health professionals are required to undertake their jobs is evolving. Traditional paper healthcare records are being replaced by electronic information, which is exposing many new vulnerabilities. Continual assessment of the environment is required to ensure that the necessary controls and safeguards are still appropriate to the circumstances being experienced in the e-health environment.

**References**


Terri Letizia BHIM, GradCertHlthInformatics
Chief Health Information Manager
Northern Health
Cooper Street
Epping VIC 3076
AUSTRALIA

Kate Wendt BMedRecAdmin, GradDipHlthServMangt_
Health Information Manager
Northern Health_
Cooper Street_
Epping VIC 3076
AUSTRALIA
Lecturer, Health Information Management_
La Trobe University, Melbourne Australia