personally controlled electronic health record (PCEHR) for Australia

see also:

- administrative aspects of Emergency Medicine in Australia
- health informatics
- Choosing an Emergency Information System
- architecture and database relationships considerations for the EHR for Emergency Departments
- Systems to ensure adequate and timely follow up of investigation results such as radiology and pathology
- clinical decision support systems (CDSS)
- Victorian Emergency Department Minimum Dataset (VEMD)

introduction

- the Australian Labour Government embarked on an Australia-wide PCEHR system designed for all Australians who wish to participate in it.
- the system is due to commence operations in July 2012 after significant controversy from the Australian health IT community and providers.

basic details of the PCEHR

- the following is derived from the AMA draft guideline April 2012
- the PCEHR system is not intended to, and should not, replace a medical practitioner’s own patient files and medical records system.
- patients voluntarily opt-in to use the system personally via the system operator directly, although doctors may assist in this process via a facilitated registration process in their practice
- patients can opt-out at any time
- the PCEHR is “owned” by the patient
- the PCEHR is fundamentally a tool for the patient to use to record and remember their health information.
- the patient has the right to determine what information is included in their PCEHR, and who is able to access how much of that information.
- on registration, the patient by default gives consent to all health providers to upload health information to their record.
- parents or guardians will remain the authorised representatives for young people aged from 14 to 18, unless the young person chooses to manage their own PCEHR by personally registering with the system operator.
- circumstances where details held in the PCEHR may be disclosed without the patient's explicit consent appear to be:
  - emergency access when they are unable to consent:
    - for any patient, including one who has applied advanced access controls that prevent access to some information in their PCEHR, and who is incapable of providing consent to PCEHR access, treating medical practitioners may gain emergency access if they make a clinical judgement that this would lessen or prevent a serious threat to an individual's life, health or safety. Such emergency
access is subject to retrospective audit. The medical practitioner is not obliged to access the PCEHR even in this circumstance.

- as authorised by law, to courts and tribunals, or for law enforcement purposes
- in the course of providing indemnity cover to a healthcare provider

- a medical practitioner is not under any duty or obligation to use the PCEHR system.
- a medical practitioner can cease using the PCEHR for some of their patients but not for others.
- a medical practitioner will not be able to see what aspects of the information the patient has chosen to hide
- a medical practitioner’s duty of care to exercise reasonable care and skill in the provision of professional advice and treatment to their patient extends to the medical practitioner’s use (accessing, disclosing, uploading) of the PCEHR.
- the PCEHR does NOT replace the taking of an adequate history directly from the patient
- medical practitioners should only access a patient’s PCEHR in the course of making a clinical decision relating to the patient’s care.
- if a medical practitioner discusses the PCEHR with their patient, it is recommended that they record that the discussion occurred in their own patient’s notes.
- medical practitioners should note on their patient’s file that their patient has consented to the medical practitioner interacting with the patient’s PCEHR every time that consent is obtained.
- good medical practice involves advising the patient you will upload information to their PCEHR
- clinical documents uploaded to the PCEHR system must be authored by a healthcare provider who has an individual healthcare provider identifier.
- those who upload patient information or Event Summaries to the PCEHR should consider how the information they choose to add will benefit subsequent users.
- if you identify erroneous or poor quality information in the PCEHR, you should inform the patient and document you have done this in your own record
- medical practitioners should not be their own Nominated Healthcare Provider for their PCEHR if they have elected to use the PCEHR system as a patient.
- the PCEHR will automatically be populated with data from:
  - Medicare Benefits Schedule
  - Pharmaceutical Benefits Scheme
  - Australian Childhood Immunisation Register
  - Australian Organ Donor Register

processes for clinicians and hospitals

- the following is based on a PECHR document in Aug 2012:
- each clinical organisation will appoint a “Responsible Officer” (RO) and a “Organisation Maintenance Officer” (OMO), the latter will perform the following functions:
  - apply for a HPI-O (Seed) for the organisation which is the organisation’s unique identifier
  - update DHS database with HPI-O data as needed
  - manage the organisation’s clinicians (who each must have their own HPI-I record and an individual PKI certificate and password for transmitting encrypted data) and authorised employees to link their Individual HI to the HPI-O of the organisation
  - updates the Healthcare Provider Directory (HPD) with the organisation details

- once PECHR-compliant software has been installed:
  - the organisation’s clinical database must be current for the patient and in particular, be able to store the clinician's HPI-I and the patient's HPI-I and these must be unique in the database, and the patient data must have accurate, current Medicare details for matching to take place.
  - the clinicians can search for a patient's HPI-I using:
personally controlled electronic health record (PCEHR) for Australia

- mandatory fields: surname, DOB, gender
- optional fields: given name, Medicare card number or DVA number, address
  - linkage of PCEHR patient record to the organisation's patient record should only be done for “verified” patient IHI's (i.e. the patient's identity has been confirmed by DHS)

- **software compliance is only possible via passing both:**
  - Notice of Connection (NOC) testing with DHS
  - Compliance, Conformance and Accreditation (CCA) testing with a NATA accredited testing laboratory

**mandatory reporting of unauthorised data access**

- “Mandatory reporting rules will apply to PCEHR data breaches, with practices and other operators of data repositories facing fines of up to $55,000 if they fail to report unauthorised access to information in a patient’s e-health record. New guidelines released by the Office of the Australian Information Commissioner (OAIC) state that e-health data repository operators must report all potential data breaches, even if they do not seem serious. Failure to report may incur a penalty of $11,000 for an individual and up to $55,000 for a body corporate. The “notifiable data breaches” apply to unauthorised collection, use or disclosure of health information in a consumer’s e-health record and events that may compromise the security or integrity of the personally controlled electronic health”

**online references**

- AMA draft guidelines for doctors on use of the PCEHR April 2012
  - direct link to pdf file


Last update: 2012/09/06 09:19