Risk Management for the PCEHR

Regulatory

Presented by:

Alison Choy Flannigan

Partner - Health, aged care & life sciences

MIIAA Annual Forum

18 October 2012

HolmanWebb Lawyers

Introduction

- Risk Management for the PCEHR - Regulatory
  - What is involved?
  - Basic Rules for healthcare providers
  - Personally Controlled Electronic Health Records Act
  - The PCEHR Rules
  - Participation Agreements
  - Privacy

2

Risk management for the PCEHR

- What is involved?
  - Regulatory requirements & the Participation Agreement
  - Recruiting patients
  - Obtaining consent
  - Comply with privacy obligations
  - Dealing with privacy related requests

3

Risk management for the PCEHR

- Basic rules for healthcare providers
  - You can opt-in or opt out at any time
  - Read and note your obligations under the Act, the PCEHR Rules and the Participation Agreement
  - When communicating with patients about the PCEHR, use the messages and information provided by DOHA
  - Understand your privacy obligations
  - Only access the records of your patients
  - Don't treat the PCEHR as a complete medical record
  - Ask the patient each time if they are happy to include the new consultation entry into their electronic record

4

Risk management for the PCEHR

- Basic rules for health care professionals
  - Respect the patient's wishes/follow their consent
  - Explain to them the risks if they don't include the information
  - Ensure that the information your practice uploads is prepared by appropriately qualified people & is accurate
  - Implement appropriate security and safety arrangements
  - Comply with privacy obligations in relation to your own medical records (which may include downloaded extracts)
  - Deal with patients request for access and correction and complaints promptly

5

Risk management for the PCEHR

- *Personally Controlled Electronic Health Records Act 2012 (Cth)*
  - S.59: Unauthorised collection, use or disclosure of health information included in a consumer's PCEHR - 120 penalty units
  - S. 61: A participant in the PCEHR system is authorised to collect, use and disclose health information included in a registered consumer's PCEHR if:
    - the collection, use or disclosure of the health information is for the purpose of providing healthcare to the registered consumer; and
    - is in accordance with access controls set by the registered consumer or if the registered consumer has not set access controls, in accordance with the default access controls (excludes consumer only notes)

6

Risk management for the PCEHR

- *Personally Controlled Electronic Health Records Act 2012 (Cth)*
  - S.64 Collection, use and disclosure in the case of a serious threat:
    - Necessary to lessen or prevent a serious threat to an individual's life, health or safety; *and*
    - It is unreasonable or impracticable to obtain consent; *and*
    - The participant must notify the System Operator of those matters; *and*
    - The collection, use or disclosure occurs not later than 5 days after that advice is given.
    - Does not authorise access to consumer-only notes.

7

Risk management for the PCEHR

- *Personally Controlled Electronic Health Records Act 2012 (Cth)*
  - S. 65: Subject to s 69, collection, use and disclosure health information included in a consumer's PCEHR if the collection, use or disclosure is required or authorised by law
  - 69 (3) Except as mentioned in subsection (1) or (2) (which relates to requests to the System Operator), a participant in the PCEHR system or a consumer cannot be required to disclose health information included in a consumer's PCEHR to a court or tribunal
  - 69 (1) permits a court order to be provided to the *System Operator* in certain circumstances, including for the provision of indemnity cover to a healthcare provider and to the coroner.

8

Risk management for the PCEHR

- *Personally Controlled Electronic Health Records Act 2012 (Cth)*
  - S 74: Registered healthcare provider organisations must ensure certain information is given to System Operator – if an individual requests access to a consumer's PCEHR on behalf or purportedly on behalf of the registered healthcare provider organisation and does not give enough information to identify the individual

9

Risk management for the PCEHR

- *PCEHR Rules 2012*
  - Healthcare provider organisations (depending upon size) must have a written policy which addressed specified matters concerning:
    - Training
    - Identifying a person who requests access
    - Physical and information security measures
    - Mitigation strategies
  - User account management
  - Retention of record codes and document codes

10

Risk management for the PCEHR

- *PCEHR (Participation Agreement) Rules 2012 (Cth)*
  - Registration is conditional upon agreement by healthcare provider organisations
  - You must take reasonable steps to ensure that you and your employees exercise due care and skill so that records uploaded and downloaded are accurate, up-to-date and not misleading or defamatory

11

Risk management for the PCEHR

- *PCEHR (Participation Agreement) Rules 2012 (Cth)*
  - You must notify the System Operator (DOHA) if:
    - you know or suspect there is a non-clinical PCEHR system-related error in a record or the security of the PCEHR system has been compromised by you, your employee or using your equipment
    - There is a material change in your legal structure or you are involved in a merger or acquisition or
    - Your contact person or their contact details change

12

Risk management for the PCEHR

- *PCEHR (Participation Agreement) Rules 2012 (Cth)*
  - You can only upload material to the PCEHR system when you own the IP rights in the material or the owner has agreed
  - At our request and on reasonable notice, you must provide reasonable assistance in relation to any inquiry, investigation or complaint, in connection with the PCEHR system conducted, handled or facilitated by DOHA
  - You warrant that, to the best of your knowledge, the information you have supplied in this agreement is accurate, complete, up-to-date and not misleading

13

Privacy

Privacy Legislation (health industry private sector)

Privacy Act 1988 (Commonwealth)

Health Records and Information Privacy Act 2002 (NSW)

Health Records Act 2001 (Vic)

Health Records (Privacy and Access) Act 1997 (ACT)

Note: The Australian Law Reform Commission Report "*For your Information: Australian Privacy Law and Practice" (ALRC 108)*

14

Privacy

- Privacy
  - Privacy controls – privacy laws; consumer consent; participation agreements for providers
  - Privacy risks
    - Obtaining adequate privacy consent – opt in and opt out models
    - Systems must give effect to patient's consent
    - Unauthorised collection - Ensuring that the only information collected is required to treat the patient
    - Unauthorised disclosure, including to consultants/cloud computing
    - Data quality – patient and provider identification & uniformity of medical terms and abbreviations
    - Data security

15

Privacy

Key concepts

"**personal information**" means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion

16

Privacy

Key concepts

"**health information**" means:

(a) information or an opinion about:

the health or disability (at any time) of an individual; or

an individual's expressed wishes about the future provision of health services to him or her; or

a health service provided, or to be provided, to an individual;

that is also personal information; or

(b) other personal information collected to provide, or in providing a health service; or

(c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body part, organs or body substances; or

(d) genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual

17

Privacy

Key concepts

"**health service**" means:

(a) an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the person performing it:

to access, record, maintain or improve the individual's health; or

to diagnose the individual's illness or disability; or

to treat the individual's illness or disability or suspected illness or disability; or

(b) the dispensing on prescription of a drug or medical preparation by a pharmacist

18

Privacy

Key concepts

Currently "employee records" are *excluded* but there are plans to include:

"**employee record**", in relation to an employee, means a record of personal information relating to the employment of the employee. Examples of personal information relating to the employment of the employee are health information about the employee and personal information about all or any of the following:

engagement; training; disciplining; resignation; termination; terms and conditions of employment; personal and emergency contact details; performance or conduct; hours of employment; salary or wages; membership of a professional or trade association; trade union membership; leave; taxation; banking or superannuation

19

Privacy

National Privacy Principles (Privacy Act)

- Collection
- Use and disclosure
- Data quality
- Data security
- Openness
- Access and correction
- Identifiers
- Anonymity
- Transborder data flows
- Sensitive information

20

Conclusion and questions

alison.choyflannigan@holmanwebb.com.au