E-health Records: How and Why the Law Must Change to Promote Better Privacy in Healthcare

Presenter

Bianca Phillips
Lawyer & Lecturer
I. Advancing healthcare through electronic health

II. Survey data on consumer and physician interest, uptake and concerns

III. The e-health records legislative framework: Strengths and Limitations

IV. In-practice tips for protecting privacy

V. Future considerations
PART I

ADVANCING HEALTHCARE THROUGH ELECTRONIC HEALTH
### Definition of e-health

<table>
<thead>
<tr>
<th>Tele-health</th>
<th>Electronic Health Records</th>
<th>The World Wide Web as an information tool</th>
<th>Compatible Health/Medical Electronic Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Electronic Health Records

The World Wide Web as an information tool

Compatible Health/Medical Electronic Devices
Hypothetical: Patient 1

- **Scenario:**
  - 45 year old teacher suffers from asthma and type 1 diabetes
  - History of acute asthma attacks resulting in hospitalisation
  - She worries about the prospect of falling ill whilst at work
  - How might e-health assist Patient 1?

Hypothetical: Patient 1

- Inhaler fitted with a sensor
- Bracelet monitoring vital signs, stored to app – sent to doctor
- Car fitted with vital signs sensor
- Car fitted with warnings for other drivers and lights to attract attention. Automatically pulls car over in emergency.
- Distress signal sent to ambulance automatically
- Glucose sensor below skin, automatic release or individual control
- Appointments made with physicians via smart phone application
- Information stored to e-health record
Hypothetical: Patient 2

**Scenario:**
- 40 year old man experiences severe abdominal distension – he is brought to the emergency department at 3am
- Family history of bowel cancer, glaucoma and heart disease
- **How might e-health assist Patient 2?**

Hypothetical: Patient 2

Step 1
Regular provider creates a shared health summary

Step 2
Patient presents to Emergency Department

Step 3
Hospital accesses e-health records

Step 4
Patient treated

Step 5
Hospital uploads discharge summary to e-health

Step 6
Patient discharged
Available technologies

- Tele-radiology
- Tele-stroke assessment (See: Victorian Stroke Telemedicine Program, running since 2007).
- Tele-psychiatry* (a very serious court case ‘Hageseth v. Superior Court’ unfolded in the USA against a physician who was sentenced to jail.)
- Wireless sensors – vital signs, continuous glucose monitoring, mood sensors, sleep monitors.
- Smart phone ECG monitors
- Portable ultrasounds
- Fax, scans, email transmissions
- Telephone and Skype consultations
- Electronic health records
PART 2

SURVEY DATA – INTEREST, UPTAKE AND CONCERNS
“There has been a steady increase in the number of downloads of smart phone applications that track health and fitness, an increase in the adoption of telemedicine/[telehealth] practices, and there have been progressive (yet small) increases in registrations of the e-health records system in Australia. However, surveys show that people remain concerned about the privacy of their health information, and this may prevent consumers from utilising these technologies.”

Concerns

United States:
- 2005 Harris Interactive study: 67% concerned about privacy of medical records generally. 70% concerned about privacy with regards to e-health records.
- 2013 Harris Interactive study: 62% not at all confident or only somewhat confident that their medical information would remain secure. 83% concerned with security of health information stored in a e-health record.

Australia:
- 2011 Newspoll survey: 41% of respondents were not confident that their details would remain confidential under the e-health records system.
Interest

United States:
- 2013 Harris Interactive poll: 1 in 3 were very or extremely interested in using smartphones or tablets to ask doctors questions, make appointments or to obtain medical test results. Older users (65+) were not as interested in using smartphones or tablets for such purposes.

Australia:
- Lack of comparative data regarding consumer interest.
- 2007 Nielsen survey: older users (65+) are more likely to use the internet to access health and medical information than the average adult population.
Globally:
- 2012 WHO survey of 114 countries: **over 40% of respondents use electronic platforms** to store and use individual patient health data. Adoption is linked to country resources.

Australia:
- At 31 July 2013: 5,060 healthcare organisations, 7,766 individual providers and 612,390 patients were registered. Some reports say that the number have risen to 900,000 patients.

Denmark:
- 98% of primary care practices use electronic medical records. Denmark is described by some as a e-health success story.
Uptake (Using health information online)

Globally:
- 2011 WHO study: 1 in 2 search health information online to self diagnose. Highest rates of this practice occur in Russia, US, UK and Australia.

United States:
- Harris Interactive 2010 survey: 53% of respondents used internet for guidance on health matters. 46% did not consult with their doctor regarding information found on the internet.
- Since 1998 gradual rise in the number of respondents looking to the internet for health information.

Australia:
- 2010 Nielsen study: searching for health and medical information online, among top 10 internet activities for 16+ year olds. 25% Australians regularly seek health information online.
Uptake (Telehealth)

- 2011 Uni-quest report: found **limited activity for telehealth in Australia**.

<table>
<thead>
<tr>
<th>Service</th>
<th>Number of consultations per year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telepaediatric service in Queensland</td>
<td>2,500</td>
</tr>
<tr>
<td>Mental health service in South Australia</td>
<td>1,800/2,000</td>
</tr>
<tr>
<td>Plastic surgery service in Western Australia</td>
<td>1,200</td>
</tr>
<tr>
<td>Tele-neurology consultations in Western Australia</td>
<td>600</td>
</tr>
</tbody>
</table>

Table 3: Number of Telehealth Consultations in Australia per year

- Globally - Increased downloads of health apps worldwide, however, not all apps are genuinely ‘health related’ – findings from a US study of 43,689 apps.
PART III

THE E-HEALTH RECORDS LEGISLATIVE FRAMEWORK FOR PRIVACY: BENEFITS AND LIMITATIONS

Cth Privacy Framework

- Personally Controlled Electronic Health Records Act 2012 (Cth)
  - 1 minor amendment due to Privacy Amendment (Enhancing Privacy Protection) Act
- Healthcare Identifiers Act 2010 (Cth)
  - Several minor amendments due to Privacy Amendment (Enhancing Privacy Protection) Act
- Privacy Act 1988 (Cth)
  - Major amendments under the Privacy Amendment (Enhancing Privacy Protection) Act (most commenced on 12 March 2014). Note – likely introduction of Binding Codes (s26A). See: Section 6 & APP 3, 4, 11.
  - Covers organisations and agencies. Organisation is defined in s 6C to include individuals.

Source: CommLaw and Office of Parliamentary Counsel.
State and Territories

- Note, State and Territories also have health records legislation. For example:
  - *Right to Information Act 2009* (Qld) (RTI Act) and *Information Privacy Act 2009* (Qld) (IP Act)
  - *Personal Information and Protection Act 2004* (Tas).

- Cth laws prevail to the extent of any inconsistency (s109 Australian Constitution)
‘At present, consumer health records are scattered over a range of locations and clinics rather than being attached to the consumer and easily available at the point of care. This means that consumers need to retell their story every time they visit a different healthcare provider. This outdated approach can result in ... unnecessary retesting, delays and medical errors.’

‘...The Personally Controlled Electronic Health Records Bill 2011 before the House today establishes the essential IT and governance infrastructure that allows consumers to set up their own personal electronic health records—computer based records that can be accessed anywhere there is an internet connection. That means that records can travel with consumers clinic to clinic and doctor to doctor at the click of a button. (emphasis added).’

‘We are very aware that this is a complex area of reform and a that a national e-health records system will have to be built over time as both consumers and healthcare providers join the system.’

Benefits

- Interacts with the Privacy Act 1988 (Cth)
- Optional (opt in)*
- Ease/convenience for patients
- Speed
- Potential for reduced error
  - See Article – Woman dies of drug overdose after hospital blunder, 12 October 2012
    http://www.abc.net.au/pm/content/2012/s3609775.htm
- A level of regulation, oversight and security.

* This may also be argued as a limitation
Limitations

1. Interacts with the Privacy Act, however, the scope of powers of the Information Commissioner to conduct an Audit for healthcare identifier numbers (the keys to the system) is unclear. See s 29(3) of Healthcare Identifiers Act.
2. The incentives for physicians are low
3. Large scale cloud storage - sensitive information and hacking
4. CEO of Medicare ‘registered repository operator’ – may disclose identifying information to the System operator. And defined as the service operator, so they have the task of allocating identifier numbers (the keys to the system)

- The role should be afforded to a constitutionally entrenched authority. That way the identity of the service operator could not be easily changed through amendment.
5. Storage for 30 years after death or 130 years.
6. Opt in – defeats many of the argued benefits e.g. Reducing error/abuse of the prescription system
7. Lack of guidance on IT governance, including audit and encryption. Server security. See s 15(g) of the PCEHR Act.
8. Independent advisory committee membership determined by the Minister. Perhaps better determined by the Governor General in Council.
9. Potential use of identifiable data for statistics when de-identified.
10. Managers of the system – either Secretary of Department or another body as determined by the Regulations (delegated) s 14 PCEHR – This has risks.
11. No guidance regarding ownership of data.
12. We cannot have legislation for each technology (solution: binding codes for services?)
Examples

Old s 29 Healthcare Identifiers Act
Functions of Privacy Commissioner
- Audits
- (3) For the purpose of paragraph 27(1)(h) of the Privacy Act 1988 (about audits), a healthcare identifier is taken to be personal information.

Old s 27(1)((h) Privacy Act:
27 Functions of Commissioner in relation to interferences with privacy (h) …. to conduct audits of records of personal information maintained by agencies for the purpose of ascertaining whether the records are maintained according to the Information Privacy Principles;

Section 27(1)(h) – repealed.
under the new privacy reforms, s 27(1)(h) has been removed and replaced with s 33C (confirmed in the EM)
Examples

Healthcare Identifiers Act (Current)
Section 29 Assessment by Information Commissioner

(3) For the purpose of paragraph 33C(1)(a) of the Privacy Act 1988, a healthcare identifier is taken to be personal information.

Privacy Act (Current)
33C Commissioner may conduct an assessment relating to the Australian Privacy Principles etc.

(1) The Commissioner may conduct an assessment of the following matters:

(a) whether personal information held by an APP entity is being maintained and handled in accordance with the following:
  - (i) the Australian Privacy Principles;
  - (ii) a registered APP code that binds the entity;
Examples

Transitional provisions (Privacy Law Amendments)

- 9 Audits by the Commissioner
- (1) This item applies if:
  (a) before the commencement time, the Commissioner was conducting an audit under paragraph 27(1)(h) or (ha), 28(1)(e) or 28A(1)(g) of the Privacy Act; and
  (b) immediately before that time, the audit has not been completed.
- (2) Despite the amendments of the Privacy Act made by this Act, the Commissioner may continue, after the commencement time, to conduct the audit as if those amendments had not been made.
The System Operator has the following functions:

....(g) to establish and maintain an audit service that records activity in respect of information in relation to the PCEHR system;
14 Identity of the System Operator

(1) The System Operator is:

(a) the Secretary of the Department; or

(b) if a body established by a law of the Commonwealth is prescribed by the regulations to be the System Operator—that body.

(2) Before regulations are made for the purposes of paragraph (1)(b), the **Minister must be satisfied** that the Ministerial Council has been consulted in relation to the proposed regulations.
17 Retention of records uploaded to National Repositories Service

... (2) The **System Operator** must ensure that the record is retained for the period:

(a) beginning when the record is first uploaded to the National Repositories Service; and

(b) ending:

(i) **30 years after the death of the consumer**; or

(ii) **if the System Operator does not know the date of death of the consumer**—130 years after the record was first uploaded to the National Repositories Service.
National Repositories Service – definition section refers you to section 15(i) for the definition:
(i) to operate a National Repositories Service that stores key records that form part of a registered consumer’s PCEHR (including the consumer’s shared health summary);
PART I

IN PRACTICE TIPS FOR IMPROVING PRIVACY
• **Health practitioners and health services**
  - Review current IT governance
  - Seek specialist IT advice.
  - Seek legal advice for clarity regarding legal obligations.

• **Patients**
  - Consider the benefits vs risks of signing up to the e-health records system. Make an informed decision.
  - Seek advice if unsure.
PART V

FUTURE CONSIDERATIONS
• IT Governance
• Accountability & Transparency
• Public confidence
• Incentives for healthcare practitioners
• Ownership of data – how do we allocate rights?
  There is an overlap in rights afforded under the Privacy Act.
• Eventually opt out