A Review of Privacy and Consent Management in Healthcare: A Focus on Emerging Data Sources

Muhammad Rizwan Asghar, TzeHowe Lee, Mirza Mansoor Baig, Ehsan Ullah, Giovanni Russello, Gillian Dobbie

Presented at the 13th IEEE International Conference on eScience - Safe Data Workshop
October 2017
Agenda

- Introduce the Precision Driven Health partnership
- Describe gaps in the consenting process in healthcare
- Discuss legislation around data privacy in healthcare
- Describe characteristics of Electronic Health Records
- Summarize state-of-the-art and highlight some of the current challenges
The PDH joint research partnership, established in 2016, is supported by the Ministry of Business, Innovation and Employment (MBIE), New Zealand.

An investment of NZ$38 million over 7 years.

Founding partners include:
- Orion Health Ltd.
- The University of Auckland
- Waitemata District Health Board (WDHB)

PDH aims to provide data-driven precision health by combining and learning from the massive volume of data, from:
- Electronic health records
- Smart devices (say wearables and smartphones)
- Social networks (say Facebook and Twitter)
- Etc.

Will use machine learning and optimisation techniques to provide more personalised healthcare plans, and improved services.
PDH Themes

1. New Data Sources (NDS)
   - Broadening the scope of precise healthcare by making NDS available

2. Predictive Modelling
   - Utilise a variety of big data sources for predictive modelling in a healthcare setting

3. Precise Healthcare
   - Utilise disparate data sources, analyses, and technologies to enable precise healthcare

4. Empowering people
   - Leverage technology to empower all people to self-manage their health
New Zealand Healthcare Data Landscape

Image Source: Galpottage and Norris, “Patient Consent Principles and Guidelines for E-Consent”
Current State of Consent

- Electronic Health Record (EHR) systems have been implemented in New Zealand.

- Health data is fragmented and stored locally by different entities including:
  - DHBs
  - ACC
  - GPs at medical centers
  - Hospitals
  - ...

- However, we still use a paper-based consent form.

- To access health data at Auckland DHB, you need to fill in a paper-based consent form and wait up to 20 working days, you will get a hard copy of medical records back.
Gap Analysis

The gaps in current state of consent are:

1. There is no avenue for patients to audit/check for what purpose, where and who is using their data.

2. There is no allowance for revocation of consent.

3. Some aspects, such as use, modification, and storage of data, are an implied consent, not explicitly stated. However, to support New Data Sources in Precision Driven Health (PDH), we require a more transparent consent.

4. Transfer from a hard copy consent to a digital consent introduces manual workload.

To understand how consent is accounted for in other jurisdictions, we went on to consider current legislation, standards and real-world systems.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Collection of data &amp; Patient’s rights</strong></td>
<td>Purpose of data collection must be specified. Patients must be adequately informed about what information is collected.</td>
<td>Individuals must be informed of the purpose, extent of data collected.</td>
<td>Detailed information of how data is being used must be made available when identifiable information is used.</td>
<td>Rights to inform patient how information is disclosed and to whom in privacy notices.</td>
</tr>
<tr>
<td><strong>Referrals/data sharing</strong></td>
<td>Use and disclosure of health information is limited to the purposes stated. Unique identifiers must be used to protect personal information.</td>
<td>Health records can only be used for the purposes stated to the patient, any secondary use must be requested unless it is an emergency.</td>
<td>There are no specific rules requesting patient consent before sharing data, although the purpose for each collection must be stated explicitly.</td>
<td>No patient authorisation needed to share data.</td>
</tr>
<tr>
<td><strong>Ability to view/correct PHR</strong></td>
<td>Patient has right to view PHR and request correction if necessary. Healthcare provider must ensure data is up-to-date. Health data must be stored for 10 years.</td>
<td>Patients can view their PHR and request to delete, change, or add data.</td>
<td>Patients are given right to view, erase and correct their PHR data.</td>
<td>Patients are given the right to view and request for corrections but healthcare providers do not have to conform.</td>
</tr>
<tr>
<td><strong>Data disclosure</strong></td>
<td>Healthcare providers must ensure adequate protection of data. Disclosure of confidential data to authorised individuals only and for consented purposes only.</td>
<td>Disclosure of data is prohibited outside of consented purpose and authorised individual.</td>
<td>Authentication mechanisms, electronic method of identification and audit logs are required.</td>
<td>Authorised access, safeguards, and breach notification specifications are addressed. Audit logs must be stored for 6 years.</td>
</tr>
</tbody>
</table>
Data collection is similar across the legislations we studied.

However, other aspects (including data sharing, viewing/updating records) differ.

Health Insurance Portability and Accountability Act (HIPAA) of US is more flexible for healthcare providers.

European Union Data Protection Directive (EU DPD) [3] is more general, does not encompass consent revocation, though it is expected to be introduced from 2018 in the General Data Protection Regulation (GDPR) [5].

Australia New South Wales Health Records and Information Privacy Act (AUS NSW HRIPA) legislation is most similar to New Zealand legislation.
US Precision Medicine Initiative (PMI)

“An approach to disease treatment and prevention that seeks to maximise effectiveness by taking into account individual variability in genes, environment, and lifestyle”.

New data sources considered include:
- Information from social networks
- Location and environment data
- Sensor data originated from phones and wearables
- Behavioural and lifestyle measures
- Organised health data from EHR
- Self-reported measures
- ...

Source: Precision Medicine Cohort Program Executive Summary
The aim of US PMI is similar to NZ PDH, however there are differences in the legislation:

- In US, healthcare providers can deny access to certain records if deemed necessary.
- In US, healthcare professionals are free to share patient info using treatment as a reason.
- Whereas, in NZ authorisation is needed for sharing EHR and it can only be used for purpose specified.
- In both US and NZ, any use of de-identified data must be disclosed.

New Zealand privacy law is more strict:

- Information acquired can only be used for the purposes stated.
- Sharing on referral is only allowed when the patient consents to sharing.
Health Information Security Framework (HISO 10029:2015)
- Defines information guidelines for health professionals dealing with personally identifiable information.
- General consent is assumed.
- Change to accommodate patient empowerment must be made.
- No provision for data from New Data Sources (NDS).

Māori Health Strategy - He Korowai Oranga
- Guides Government and healthcare sector to achieve best outcomes for Māori
- Treaty of Waitangi and Māori culture studied to see if special provision was needed.
- Importance of whānau and sharing before making medical decision.
- Provide whānau access to EHR.
## Existing EHR Systems

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pseudo-anonymity</strong></td>
<td>National Health Index (NHI) number</td>
<td>No anonymity measures in place</td>
<td>De-identified using national identification number</td>
<td>No anonymity measures in place</td>
<td>No anonymity measures in place</td>
<td>Data is de-identified before update to blockchain</td>
</tr>
<tr>
<td><strong>Data encryption</strong></td>
<td>Data stored is not encrypted</td>
<td>Data transfer is encrypted using PKI</td>
<td>Data is not encrypted</td>
<td>Data is not encrypted</td>
<td>Data is not encrypted</td>
<td>Not mentioned</td>
</tr>
<tr>
<td><strong>Authentication framework</strong></td>
<td>Pre-assigned roles to healthcare provider</td>
<td>Registration with identity provider service</td>
<td>Pre-assigned roles to healthcare provider</td>
<td>Healthcare provider with smart card</td>
<td>Healthcare provider with smart card</td>
<td>Smart contract PKI</td>
</tr>
<tr>
<td><strong>Access control</strong></td>
<td>Role-Based Access Control</td>
<td>Only available to personnel with PAC</td>
<td>Role-Based Access Control</td>
<td>Identity-based + smart card</td>
<td>Identity-based + smart card</td>
<td>Blockchain smart contracts</td>
</tr>
<tr>
<td><strong>Emergency access rules</strong></td>
<td>-</td>
<td>Healthcare provider can use &quot;break-glass&quot; feature to access data</td>
<td>Not defined, healthcare provider can access all data</td>
<td>Healthcare provider can use &quot;break-glass&quot; feature to access data</td>
<td>Not mentioned</td>
<td>Not mentioned</td>
</tr>
<tr>
<td><strong>Consent granting and revocation</strong></td>
<td>Patients can opt-out</td>
<td>Using PAC delivered to user mobile</td>
<td>Not available</td>
<td>Patients can opt-out</td>
<td>Patients can opt-out</td>
<td>Yes, using smart contract</td>
</tr>
<tr>
<td><strong>Audit log</strong></td>
<td>Available only to administrator</td>
<td>Available to patients and administrator</td>
<td>Available only to administrator and privacy officer</td>
<td>Available only to administrator</td>
<td>Available only to administrator</td>
<td>Available to all, public ledger of transactions</td>
</tr>
</tbody>
</table>
Summary of Existing Systems

- Except for Australia, all other countries have:
  - No option for patient to access or control their EHR.
  - Dynamic digital consent is not present.
  - No patient accessible logs.

- Australia is the closest in terms of fulfilling
  - Privacy requirements,
  - Unification of records, and
  - Empowering patients.
Some Suggestions

In light of the gap that was highlighted, we suggest:

1. Unification of healthcare data with the EHR.
2. Allow patient access and control over healthcare data.
3. Implementation of dynamic digital consent.
4. Provide data protection for storage and transmission.
Research Challenges

- Dynamic consent collection mechanism
  - Consent must be presented in a way that is transparent, useable, flexible, and dynamic for patients.
  - Patients should be notified about their data being accessed without too much intervention.

- Access for other stakeholders to healthcare data
  - Consent should also cover other parties, such as government organisations and insurance companies.

- Privacy consideration for New Data Sources (NDS)
  - NDS is fragile in nature and disclosure should be determined by the patients.
  - Capturing consent could be different from EHR and should be revocable at any time.
  - Consideration of legal, technical and regulatory requirements, and usability aspects must be taken into account.
Thank you!
Questions?
References


References (2)


