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

THE UNIVERSITY OF AUCKLAND NEW ZEALAND

PRECISION DRIVEN HEALTH

ORION HEALTH

AUCKLAND DISTRICT HEALTH BOARD Te Toka Tumai

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

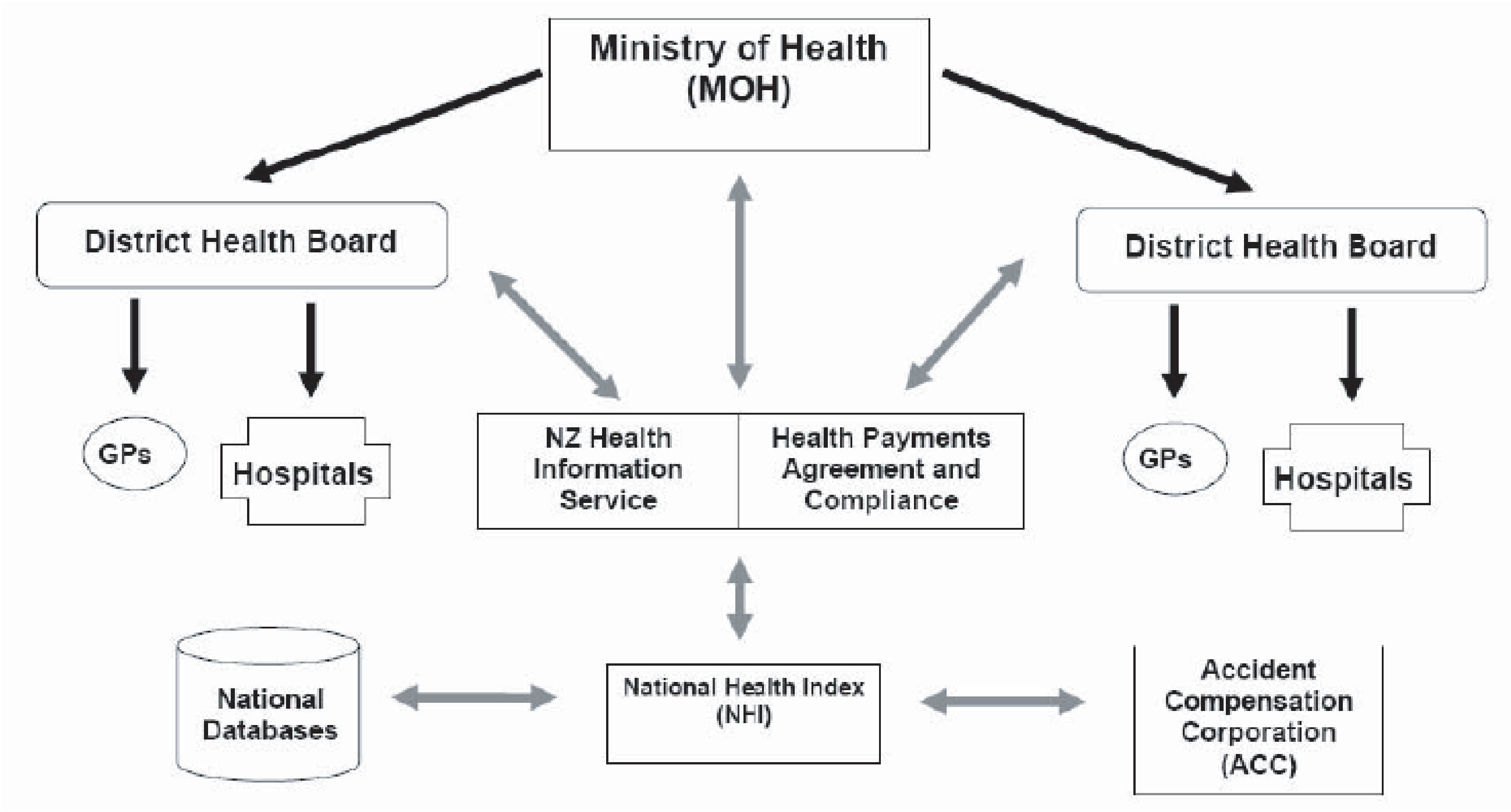
Precision Driven Health (PDH)

- 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

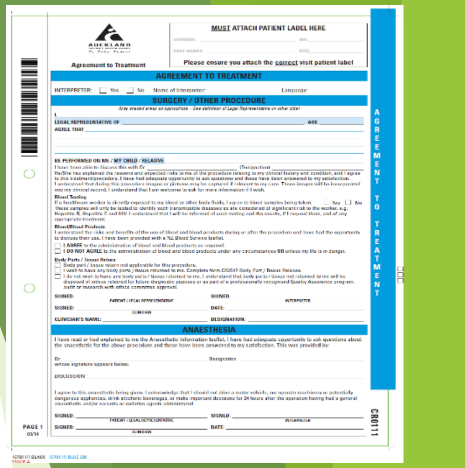


Ministry of Health (MOH)
District Health Board
District Health Board
GPs
Hospitals
NZ Health Information Service
Health Payments Agreement and Compliance
GPs
Hospitals
National Databases
National Health Index (NHI)
Accident Compensation Corporation (ACC)

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.



AUCKLAND

Agreement to Treatment

MUST ATTACH PATIENT LABEL HERE

SURNAME: NHI:

FIRST NAMES: DOB:

Please ensure you attach the correct visit patient label

AGREEMENT TO TREATMENT

INTERPRETER: □ Yes □ No Name of Interpreter: Language:

SURGERY / OTHER PROCEDURE

(Use shaded areas as appropriate – See definition of Legal Representative on other side)

I,

LEGAL REPRESENTATIVE OF AGE

AGREE THAT

BE PERFORMED ON ME / MY CHILD / RELATIVE

I have been able to discuss this with Dr (Designation)

He/She has explained the reasons and expected risks to me of the procedure relating to my clinical history and condition, and I agree to this treatment/procedure. I have had adequate opportunity to ask questions and these have been answered to my satisfaction.

I understand that during this procedure images or pictures may be captured if relevant to my care. These images will be incorporated into my clinical record. I understand that I am welcome to ask for more information if I wish.

Blood Testing

If a healthcare worker is directly exposed to my blood or other body fluids, I agree to blood samples being taken. □ Yes □ No

These samples will only be tested to identify such transmissible diseases as are considered of significant risk to the worker, e.g. Hepatitis B, Hepatitis C and HIV. I understand that I will be informed of such testing and the results, if I request them, and of any appropriate treatment.

Blood/Blood Products

I understand the risks and benefits of the use of blood and blood products during or after the procedure and have had the opportunity to discuss their use. I have been provided with a NZ Blood Service leaflet.

□ **I AGREE** to the administration of blood and blood products as required.

□ **I DO NOT AGREE** to the administration of blood and blood products under any circumstances **OR** unless my life is in danger.

Body Parts / Tissue Return

□ Body part / tissue return not applicable for this procedure.

□ I wish to have any body parts / tissue returned to me. Complete form CR6547 Body Part / Tissue Release.

□ I do not wish to have any body parts / tissue returned to me. I understand that body parts / tissue not returned to me will be disposed of unless retained for future diagnostic purposes or as part of a professionally recognised Quality Assurance program, audit or research with ethics committee approval.

SIGNED: PATIENT / LEGAL REPRESENTATIVE SIGNED: INTERPRETER

SIGNED: CLINICIAN DATE:

CLINICIAN'S NAME: DESIGNATION:

ANAESTHESIA

I have read or had explained to me the Anaesthetic Information leaflet. I have had adequate opportunity to ask questions about the anaesthetic for the above procedure and these have been answered to my satisfaction. This was provided by:

Dr Designation

whose signature appears below.

DISCUSSION

I agree to this anaesthetic being given. I acknowledge that I should not drive a motor vehicle, nor operate machinery or potentially dangerous appliances, drink alcoholic beverages, or make important decisions for 24 hours after the operation having had a general anaesthetic and/or narcotic or sedative agents administered.

SIGNED: PATIENT / LEGAL REPRESENTATIVE SIGNED: INTERPRETER

SIGNED: CLINICIAN DATE:

PAGE 1
03/14

CR0111

AGREEMENT TO TREATMENT

(CR0111) BLACK (CR0111) BLUE 299
PROOF A

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**.

Legislation in various countries

Concerns	NZ HIPC 1994 [1]	AUS NSW HRIPA [2]	EU DPD [3]	US HIPAA [4]
***Collection** of data & Patient's rights*	Purpose of data collection must be specified. Patients must be adequately informed about what information is collected.	Individuals must be informed of the purpose, extent of data collected.	Detailed information of how data is being used must be made available when identifiable information is used.	Rights to inform patient how information is disclosed and to whom in privacy notices.
*Referrals/data **sharing***	Use and disclosure of health information is limited to the purposes stated. Unique identifiers must be used to protect personal information.	Health records can only be used for the purposes stated to the patient, any secondary use must be requested unless it is an emergency.	There are no specific rules requesting patient consent before sharing data, although the purpose for each collection must be stated explicitly.	No patient authorisation needed to share data.
*Ability to **view/correct** PHR*	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	Patients can view their PHR and request to delete, change, or add data.	Patients are given right to view, erase and correct their PHR data.	Patients are given the right to view and request for corrections but healthcare providers do not have to conform.
*Data **disclosure***	Healthcare providers must ensure adequate protection of data. Disclosure of confidential data to authorised individuals only and for consented purposes only.	Disclosure of data is prohibited outside of consented purpose and authorised individual.	Authentication mechanisms, electronic method of identification and audit logs are required.	Authorised access, safeguards, and breach notification specifications are addressed. Audit logs must be stored for 6 years.

Summary of Legislation

- 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

New Data Sources

Social media

Banking

Shopping

Medical sensors

Location

ANZ
countdown

US PMI vs NZ PDH

- 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**.

National Standards

- 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 Governement 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

Property	New Zealand [6]	Australian NHS [7]	Singapore NEHR [8]	UK NHS [9]	Italian NHS [10]	MedRec (US) [11]
Pseudo-anonymity	National Health Index (NHI) number	No anonymity measures in place	De-identified using national identification number	No anonymity measures in place	No anonymity measures in place	Data is de-identified before update to blockchain
Data encryption	Data stored is not encrypted	Data transfer is encrypted using PKI	Data is not encrypted	Data is not encrypted	Data is not encrypted	Not mentioned
Authentication framework	Pre-assigned roles to healthcare provider	Registration with identity provider service	Pre-assigned roles to healthcare provider	Healthcare provider with smart card	Healthcare provider with smart card	Smart contract PKI
Access control	Role-Based Access Control	Only available to personnel with PAC	Role-Based Access Control	Identity-based + smart card	Identity-based + smart card	Blockchain smart contracts
Emergency access rules	-	Healthcare provider can use "break-glass" feature to access data	Not defined, healthcare provider can access all data	Healthcare provider can use "break-glass" feature to access data	Not mentioned	Not mentioned
Consent granting and revocation	Patients can opt-out	Using PAC delivered to user mobile	Not available	Patients can opt-out	Patients can opt-out	Yes, using smart contract
Audit log	Available only to administrator	Available to patients and administrator	Available only to administrator and privacy officer	Available only to administrator	Available only to administrator	Available to all, public ledger of transactions

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

- [1] “Health Information Privacy Code 1994,” *Health Information Privacy Code 1994*. Available: https://www.privacy.org.nz/assets/Files/Codes-of-Practice-materials/HIPC-1994-2008-revised-edition.pdf [Last accessed: 26 May 2017].
- [2] “Health Records and Information Privacy Act 2002 No 71 - NSW Legislation.” Available: http://www.legislation.nsw.gov.au/#/view/act/2002/71/part1/sec6 [Last accessed: 08 June 2017].
- [3] Office for Civil Rights (OCR), “Summary of the HIPAA Privacy Rule,” May 2008, Available: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html [Last accessed: 26 May 2017].
- [4] “Directive 95/46/EC EU,” *Official Journal L 281, 23/11/1995 P. 0031 - 0050*. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML [Last accessed: 26 May 2017].
- [5] "Regulation (EU) 2016/679", *Reform of Directive 95/46/EC*, 2017. [Online]. Available: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf [Last Accessed: 09- Aug- 2017].

References (2)

- [6] P. A. B. Galpottage and A. C. Norris, “Patient consent principles and guidelines for e-consent: a New Zealand perspective,” *Health Informatics Journal*, vol. 11, no. 1, pp. 5–18, Mar. 2005.
- [7] My Health Record | Managing access, privacy and security. [Last accessed: 26 April 2017]. Available: https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/Content/privacy
- [8] Sinha P, Sunder G, Bendale P, Mantri M, Dande A. Singapore’s NEHR. In: Electronic Health Record , John Wiley & Sons, Inc.; 2012. p. 259–66.
- [9] "Summary Care Records (SCR)". [Last accessed: 26 April 2017]. Available: https://digital.nhs.uk/summary-care-records
- [10] “Italy electronic healthcare records”. [Last accessed: 26 April 2017]. Available: http://support.fascicolo-sanitario.it/guida/informazioni-utili/tutela-della-privacy-e-consensi/consenso-alla-consegna-online-dei-referti
- [11] Ekblaw A, Azaria A, Halamka JD, Lippman A. A Case Study for Blockchain in Healthcare:“MedRec” prototype for electronic health records and medical research data.