Research using electronic health records: Balancing confidentiality and public good

Katharine A. Wallis MBChB, MBHL, PhD, FRNZCGP;[1] Kyle S. Eggleton MBChB, MMSc, FRNZCGP;[1] Susan M. Dovey MPH, PhD, FRNZCGP(Hon);[2,3] Sharon Leitch MBChB, PG Dip GP, FRNZCGP;[2] Wayne K. Cunningham MBChB, MGP, MD, FRNZCGP;[3] Martyn I. Williamson MBBS, FRNZCGP[2]

[1] University of Auckland, Department of General Practice and Primary Health Care, Auckland, New Zealand

[2] University of Otago, Dunedin School of Medicine, Dunedin, New Zealand

[3] Royal College of Surgeons in Ireland - Medical University of Bahrain, Bahrain

ABSTRACT

General practitioners are increasingly approached to participate in research and share de-identified patient information. Research using electronic health records has considerable potential for improving the quality and safety of patient care. Obtaining individual patient consent for the use of the information is usually not feasible. In this article we explore the ethical issues in using personal health information in research without patient consent including the threat to confidentially and the doctor-patient relationship, and we discuss how the risks can be minimised and managed drawing on our experience as general practitioners and researchers.

Introduction

Negotiating the tension between releasing patient information for research and protecting privacy and confidentiality is the subject of considerable debate and has recently been identified as a top priority for primary care patient safety research.[1–5]

Electronic health records

Electronic health records are widespread in primary care; personal health information may be accessible to a multitude of providers often including administrative staff, healthcare assistants, and external providers. Much electronic health information is encoded using the READ or SNOMED CT coding systems. De-identified coded data are routinely extracted for quality assurance and funding purposes. Electronic health records are a valuable resource for research to ensure the safety and quality of healthcare: the coded data may be used in research linking large datasets of anonymised health information (Big Data projects) and in real-world trials, and the un-coded data (including the free-text of the daily record) may be used in research using emergent data mining software to identify targeted information or in records review projects where researchers scroll through the records.

Privacy: the legislative landscape

Patients have a right to health information privacy that stems from the principle of autonomy and concerns the right of an individual to control information about her- or himself. Most democratic countries have laws protecting patients' right to health information privacy, with consent the usual protection. When asked, most people approve the use of their health information in research.[6,7] However, time and cost constraints mean it is usually not feasible to ask.

The right to privacy is important but never absolute; there are many exceptions when doctors are legally permitted to share patient information without consent, usually in the best interests of the patient or public. There is considerable international variation in the laws, policies and protocols that govern health information and who has access to what.[8–12] In New Zealand, for example, auditors of the National Cervical Screening Programme may access patients' primary care records without consent.[13] In the European Union, the recently introduced General Data Protection Regulation gives consumers more control over how their personal information is used (patients can opt-out of sharing identifiable but not anonymised health information for research) and

J PRIM HEALTH CARE
2018;10(4):288–291.
doi:10.1071/HC18040
Published online 19 December 2018

CORRESPONDENCE TO:
Katharine A. Wallis
Department of General Practice & Primary Health Care, University of Auckland, 261 Morrin Road, Auckland 1072, New Zealand
k.wallis@auckland.ac.nz

CSIRO Publishing
Journal Compilation © Royal New Zealand College of General Practitioners 2018
This is an open access article licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

imposes on general practitioners (GPs) increased responsibility to communicate how health information may be used and to demonstrate compliance with data protection processes.[14]

Confidentiality: the ethical duty

Doctors receive private information in the course of a confidential relationship and make an implicit promise to protect the information and use it only to serve the interests of the patient. While the law might permit or even oblige doctors to share patient information, doctors have an enduring ethical duty to protect the information they have been entrusted with. Patients need to trust their practitioner if they are to disclose sensitive information and receive appropriate care.

But confidentiality is not the only important ethical duty: doctors also have a duty to provide safe and effective healthcare. Research is essential to safe and effective healthcare. Doctors also have a duty, then, to support research that seeks to build the evidence base. The duty to share information to support safe and effective healthcare may be as important as the duty to protect confidentiality.[15]

The SHARP records review project

We conducted a retrospective records review study in general practice to identify and describe patient harms: the SHARP study (Safety, Harms And Risk reduction Project).[16] Eight GP reviewers reviewed three years of de-identified electronic health records from 9000 randomly selected patients. The focus of the study was on harm, not error, defined as the physical or emotional negative consequences arising from healthcare.[17] Data included the free-text daily record, prescriptions, test results, and letters from specialists and hospital admissions. Name recognition software was used to strip names and addresses from extracted records. De-identified data were allocated to reviewers living and working in geographical locations remote from study practices. Reviewers accessed the data via a secure password protected website. Consent to participation was sought not from individual patients, but from general practices. Ethical approval was provided by the University of Otago Human Ethics Committee (HD14/32). The study was approved by the Minister of Health as a protected Quality Assurance Activity (2015/23), barring the use of research data in civil liability proceedings and providing legal immunity to both general practices and researchers.[18]

We randomly selected 72 practices nationally and invited the 62 eligible practices to participate.[19] Forty-five practices agreed (73%). The most common reasons for non-participation were commitment to confidentiality, concern about secondary use of data for financial gain, and fear of accountability repercussions. Data de-identification and security processes minimised the risks and legal protections barred misuse and secondary use of data, but GPs had no way of checking and had to decide on trust. We found GPs were more likely to trust (and to participate) if they had pre-existing relationships with or deemed the researchers trustworthy.

We found that electronic GP records were a rich source of data for studying the epidemiology of patient harms and identifying lessons to improve the patient safety. The data de-identification processes worked most of the time but were not perfect: occasionally the name of a practice, clinician, or patient remained in the extracted data. The name recognition software was more likely to fail when a name was uncommon or had atypical spelling. Deductive identification (where the free-text holds clues to the person, place or provider) was also sometimes possible even though we allocated data to reviewers geographically remote from the data source. Deductive identification is perhaps not unexpected in a country of only 4.5 million people. No identifiable data were ever passed on or misused. SHARP reviewers were all experienced GPs well versed in acting according to professional obligations. It was not possible for reviewers to contact and inform patients who had been identified because reviewers did not have contact details and also could not identify the patient's practice or doctor. Participating practices had been informed during the consent process that despite our best efforts '*some potentially identifying data are nevertheless likely to appear from time to time (eg in hospital discharge summaries)*'.

Minimising and managing the risks

Research using electronic health records often depends upon trust: doctors will only consent to research if they trust the researchers and the research. Research ethics committees have a role in ensuring the potential benefits of a project justify the risks. Good research practices including reliable data anonymisation and security processes are important. Researchers also need to maintain strong communication links with both the public and clinicians. Many patients lack awareness and understanding about the potential uses of health information, the protections in place, and how sharing information can benefit themselves and others.[20] Researchers can help to increase public understanding about the potential benefits of research and the potential dangers in not learning from the data by engaging in public education and debate.

Doctors and practices have a responsibility to communicate to enable patients to understand what information is being collected, how it will be stored and protected, how it may be used, and their rights including when and how they can opt-out. Communication with patients could be through information on practice websites, information provided on enrolment, personal communication, and clearly visible signage in practice waiting rooms. Practices could choose to give patients the opportunity to provide broad agreement to the use of their information in research, for example on enrolment. Any consent should be meaningful: informed, freely given, and a clear indication of agreement rather than implied through inaction or a pre-ticked box. Practices could offer some sort of formal data use agreement whereby patients can select the types of information (de-identified, encoded) they are willing to share with whom and for what purpose. Ideally such agreements would include the ability for patients to change their selection at any time. The opportunity to opt-out affords patients some control over the use of their information, but it risks introducing selection bias into research. It may be necessary for some practices, for example practices dealing with especially sensitive sexual or mental health information, to always require explicit patient consent to research projects.

Conclusion

Electronic health records are a rich source of data for research to improve patient care. Individual patient consent to research using electronic health data is usually not feasible. Research using personal health information without consent risks damaging the doctor-patient relationship. The risks may be minimised and managed through rigorous data anonymisation and security processes; clear communication to patients about the potential uses of health information, the protections in place, and the potential benefits of sharing information for research; and through developing mutual understanding and trust between GPs and researchers. Our experience emphasises the importance of on-going software improvements and supporting the professionalism of researchers.

References

1. McDonald L, Lambrelli D, Wasiak R, et al. Real-world data in the United Kingdom: opportunities and challenges. BMC Med. 2016;14(1):97. doi:10.1186/s12916-016-0647-x
2. Kostkova P, Brewer H, de Lusignan S, et al. Who owns the data? Open data for healthcare. Front Public Health. 2016;4(7):7.
3. Wellcome Trust. Towards consensus for best practice: use of patient records from general practice for research. London, 2009. [cited 2018 March 4]. Available from: https://wellcome.ac.uk/sites/default/files/wtx055661_0.pdf.
4. New JP, Leather D, Bakerly ND, et al. Putting patients in control of data from electronic health records. BMJ. 2018;360:j5554. doi:10.1136/bmj.j5554
5. Carter P, Laurie GT, Dixon-Woods M. The social licence for research: why care.data ran into trouble. J Med Ethics 2015;41(5):404–9. doi:10.1136/medethics-2014-102374
6. Wellcome Trust. Summary report of qualitative research into public attitudes to personal data and linking personal data. 2013. [cited 2017 October 3]. Available from: http://www.wellcome.ac.uk/stellent/groups/corporatesite/@msh_grants/documents/web_document/wtp053205.pdf.
7. Mello MM, Lieou V, Goodman SN. Clinical trial participants' views of the risks and benefits of data sharing. N Engl J Med. 2018;378(23):2202–11. doi:10.1056/NEJMsa1713258
8. Wellcome Trust. Understanding patient data. 2017. [cited 2018 March 4]. Available from: https://understandingpatientdata.org.uk/.
9. Privacy Act 1988, Stat. 119 (Australia). 1988. [cited 2017 October 17]. Available from: https://www.legislation.gov.au/Series/C2004A03712.
10. Privacy Act 1993, Stat. 28 (NZ). 1993. [cited 2012 October 15]. Available from: http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html?search=ts_act_privacy_resel8p=18sr=1.
11. Health Information Privacy Code 1994, Stat. (NZ). 1994. [cited 2012 October 15]. Available from: http://www.privacy.org.nz/health-information-privacy-code/.

12. Health Insurance Portability and Accountability Act (HIPAA) 1996, Stat. 1936 (US). 1996. [cited 2017 October 19]. Available from: https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.
13. Wallis K. Cervical screening legislation is unethical and has the potential to be counter-productive. N Z Med J. 2007;120(1266):U2840.
14. NHS Digital. General Data Protection Regulation (GDPR) guidance. UK. 2018. [cited 2018 May 23]. Available from: https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance.
15. National Data Guardian. Dame Fiona Caldicott. Review of data security, consent and opt-outs. UK: Govt. of UK. 2016. [cited 2018 April 30]. Available from: https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs.
16. Dovey SM, Leitch S, Wallis KA, et al. Epidemiology of patient harms in New Zealand: Protocol of a General Practice records review study. JMIR Res Protoc. 2017;6(1):e10. doi:10.2196/resprot.6696
17. Runciman W, Hibbert P, Thomson R, et al. Towards an international classification for patient safety: key concepts and terms. Int J Qual Health Care. 2009;21(1):18–26. doi:10.1093/intqhc/mzn057
18. Health Practitioners Competence Assurance Act 2003, Stat. 48 (NZ). 2003. [cited 2012 October 15]. Available from: http://www.legislation.govt.nz/act/public/2003/0048/latest/DLM203312.html?search=ts_act_health+practitioners_resel8p=18sr=1.
19. Leitch S, Dovey S, Wallis KA, et al. Characteristics of a stratified random sample of New Zealand general practices. J Prim Health Care. 2018;10(2):114–24. doi:10.1071/HC17089
20. Hill EM, Turner EL, Martin RM, et al. "Let's get the best quality research we can": public awareness and acceptance of consent to use existing data in health research: a systematic review and qualitative study. BMC Med Res Methodol. 2013;13(1):72. doi:10.1186/1471-2288-13-72

ACKNOWLEDGEMENTS
Health Research Council of New Zealand funded the research (HRC 14/185). Andrew McMenamin, Murray Tilyard, David Reith, Ari Samaranayaka, and Steven Lillis collaborated in the research.

COMPETING INTERESTS
Authors declare there are none.