The Safe and Effective Use of Shared Data Underpinned by Stakeholder Engagement and Evaluation Practice

A Position Paper from the IMIA Technology Assessment & Quality Development in Health Informatics Working Group and EFMI Working Group for Assessment of Health Information Systems

Andrew Georgiou[1], **Farah Magrabi**[1], **Hannele Hyppönen**[2], **Zoie Shui-Yee Wong**[3], **Pirkko Nykänen**[4], **Philip J. Scott**[5], **Elske Ammenwerth**[6], **Michael Rigby**[7]

[1] Macquarie University, Australian Institute of Health Innovation, Sydney, Australia
[2] National Institute for Health and Welfare, Information Department, Helsinki, Finland
[3] St. Luke's International University, Tokyo, Japan
[4] University of Tampere, Faculty of Natural Sciences, Tampere, Finland
[5] University of Portsmouth, Centre for Healthcare Modelling and Informatics, Portsmouth, United Kingdom
[6] UMIT, University for Health Sciences, Medical Informatics and Technology, Institute of Medical Informatics, Hall in Tyrol, Austria
[7] Keele University, School of Social Science and Public Policy, Keele, United Kingdom

Summary

Objectives: The paper draws attention to: i) key considerations involving the confidentiality, privacy, and security of shared data; and ii) the requirements needed to build collaborative arrangements encompassing all stakeholders with the goal of ensuring safe, secure, and quality use of shared data.

Method: A narrative review of existing research and policy approaches along with expert perspectives drawn from the International Medical Informatics Association (IMIA) Working Group on Technology Assessment and Quality Development in Health Care and the European Federation for Medical Informatics (EFMI) Working Group for Assessment of Health Information Systems.

Results: The technological ability to merge, link, re-use, and exchange data has outpaced the establishment of policies, procedures, and processes to monitor the ethics and legality of shared use of data. Questions remain about how to guarantee the security of shared data, and how to establish and maintain public trust across large-scale shared data enterprises. This paper identifies the importance of data governance frameworks (incorporating engagement with all stakeholders) to underpin the management of the ethics and legality of shared data use. The paper also provides some key considerations for the establishment of national approaches and measures to monitor compliance with best practice.

Conclusion: Data sharing endeavours can help to underpin new collaborative models of health care which provide shared information, engagement, and accountability amongst all stakeholders. We believe that commitment to rigorous evaluation and stakeholder engagement will be critical to delivering health data benefits and the establishment of collaborative models of health care into the future.

Keywords

Confidentiality; computer security; informed consent; evidence-based practice; program evaluation

Yearb Med Inform 2018:25-8
http://dx.doi.org/10.1055/s-0038-1641192

1 Introduction

Since the beginning of this century, an ever-greater proportion of personal and professional information has been digitally archived by the business and public sectors, including by health care services. This increasing volume of data can take a variety of forms compiled in differing formats and with divergent properties. These types of data, generally referenced as *big data,* are typically characterised by their "V" properties, namely: *volume* (the amount of data), *velocity* (the speed of data transaction and accumulation), *variety* (the range of data types and sources), *veracity* (the trustworthiness of data sources), *value* (its relevancy to health topics), and *variability* (the changing nature of health events) [1]. Additional "V" properties can include *visualisation* (representation) and *volatility* (how long the data are valid) [2]. Some view *big data* as essentially combining data from independent and very different sources, such as retail pharmacy over the counter (OTC) sales and primary care consultations, while pooled health data are seen differently as *very large data*, but for this paper the underlying issues are largely similar.

The use of large shared data sources has the potential to improve our understanding of the breadth and course of health care delivery [3], by helping to: a) identify emerging health issues and the factors that contribute to medical conditions; b) assess the safety of treatment options; c) measure the effectiveness and efficiency of health care [4, 5]; and d) improve practical and organisational effectiveness in delivery [6]. The expansion of shared data sources has also spurred the growth of *personalised medicine* with its promise of targeted molecular tests and therapies, providing a bridge between the world of clinical practice and that of molecular bioinformatics [7].

Nevertheless, there are major concerns about the extent of community awareness and individual consent to the utilisation of large shared data enterprises. The technological ability to merge, link, re-use, and exchange data has outpaced the establishment of policies, procedures, and processes to monitor the ethics and legality of shared use of data. Questions remain about how to guarantee the security of shared data [8], and how to establish and maintain public trust across large-scale shared data enterprises.

2 An Evaluation Imperative

The delivery of health care has become increasingly intertwined with the development and utilisation of new, more powerful, and more complex information systems. This means that the emergence of any problems associated with these systems (e.g. concerns about the quality and validity of data, and the security and privacy of information) is likely to impact on the provision of care and people's well-being [9]. Recent examples of data breaches of high profile data, including ransomware cyber-attacks, can adversely affect public trust [10]. The digitisation of information in health systems is a global activity. As such its progress and outcomes need to be underpinned by the evaluation and generation of: i) evidence about its effectiveness, security, and trustworthiness; and ii) robust and validated governance (e.g., what is permitted?) and security (e.g., is it effectively protected?) mechanisms [11-13].

The International Medical Informatics Association (IMIA) Working Group (WG) for Technology Assessment and Quality Development and the European Federation for Medical Informatics (EFMI) Working Group for Assessment of Health Information Systems seek to raise awareness regarding evaluation as an essential activity required to protect all stakeholders (e.g. patients and health care professionals) confidentiality, privacy, security, and safety, stimulate optimisation, and enhance sustainability [14, 15]. In a previous Yearbook submission [16], the WG enunciated some key evaluation considerations for secondary uses of clinical data, including describing a methodological framework for best practice. In this paper, we draw upon existing research and policy approaches to highlight a number of key evaluation considerations for establishing public trust in shared data involving:

- *Privacy* – an individual's right to keep information to oneself and to consent to what information is collected and how it is used [17];
- *Confidentiality* – to prevent data from being exposed to unauthorised parties [18];
- *Security* – Confidentiality, integrity (the ability to ensure that data is an accurate and unchanged representation of the original secure information), and availability (data is accessible to those who are authorised to access/process/disclose) [18].

3 Data Governance Requirements

In 2017, the Organisation for Economic Cooperation and Development (OECD) report "New Health Technologies – Managing Access, Value and Sustainability", noted that the sharing of personal health data presented a number of risks to individual privacy, which can undermine public confidence in social institutions [19]. Most of the risks of data misuse and threats to privacy occur not through the controlled sharing of data or in the release of non-identifiable data, but from hacking or other breaches that have exposed weaknesses in the collection, storage, security, and management of data [4].

It is quite reasonable to assume that there may not be a means to completely guarantee the security of all systems. As a recent *New England Journal of Medicine* commentary by Gordon and colleagues noted, as long as there is value in information, we can expect to see attacks on the systems designed to protect security [9]. Our ability to recognise the nature and public health implications of these threats is therefore critically important to improving dialogue, incorporating the views of the individual (citizen, clinician, health professional), health care organisations, and the broader community, and implementing the means to enhance trust and security [20].

Such considerations have prompted many to advocate for fundamental data governance structural changes to address today's data sharing reality [4, 20, 21]. This involves major discussions about how data is collected, stored, aggregated, linked, and transmitted [22]. For instance, when data is collected and stored for future use, it is impossible to anticipate all the potential future uses [23]. Some of the broad criteria for data governance frameworks must include the need to deliver *benefits* to the community, increase the availability and *usefulness* of data, and engender stakeholder engagement and community *trust* and *confidence* about how data are managed and used [4].

Establishing stakeholder engagement means more than guaranteeing that people have a choice, and consent to the use of their own data. It also involves: i) ensuring that consent issues related to shared data are understood; ii) promoting public awareness about the uses of shared data; and iii) engaging people in ongoing discussions about privacy, confidentiality, and security of shared data [8]. In this regard, the United Kingdom Department of Health has emphasized that the safe use of data and technology must include transparency about the governance of data, as a means of helping people make informed choices about the use of their data and its protection especially when dealing with sensitive and confidential personal health data [24].

The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data is one of the most widely recognised and commonly used privacy frameworks. Some core principles, such as collection

limitation, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability, have laid the groundwork for countries to design their own privacy and security guidelines. Revisions undertaken in 2013 have incorporated national privacy strategies, privacy management programmes, and data security breach notification into the framework [25].

Health information privacy measures should be devised to protect individuals' interests and respect intrinsic values. The collection, storage, and use of personal information as well as the justifications for sharing data need to be closely scrutinised. For instance, there should be no disclosure of potential identifiers to unauthorised parties. In some cases, pseudo-identities can be generated to replace the true identities to ensure the data can no longer be linked to their corresponding nominative identities. In every situation, it is essential to ensure minimal risk of assocating data with individual patient and staff identity.

4 National Approaches to Monitoring Compliance with Evidence-based Best Practices

Generally, when large national health IT and/or large-scale data sharing initiatives are announced, they are associated with the release of a *benefit realisation framework* designed to measure and enunciate the achievements of the initiative and plans. Many contemporary eHealth plans specify a data sharing element in their frameworks, considering either data sharing between health care providers or data sharing between health care providers and the patient. Thus, monitoring the existence and focus of these data sharing policies can provide a foundation for more detailed measurement of data sharing (e.g. see also [26]).

The prerequisite for establishing value in any data sharing exercise is that the data is available and usable by those who need it. When data is collected and stored for reuse in an electronic format, it is possible to examine usage logs to monitor who has accessed the data and the role (s)he performs [27]. From a clinical perspective, data safety and security-related competence measures (including the ability to provide assurance of confidentiality, access control, and security) have been included in a number of clinical areas (e.g. the Tiger initiative) [28], and as part of the Finnish national usability survey for nurses [29]. Other relevant evaluation measures may include: a) the proportion of professionals having access to shared data; b) the number of patient visits where shared data are used; and c) the usability and user satisfaction involved with data sharing [30]. The proportion of citizens experiencing trust as a barrier for sharing their health data has been monitored e.g., in Finland [31] as a citizen-focused measure. The status of the implementation of safety standards is one of the measures that provides a distinctive health care organisational viewpoint [32].

From a statistical and research angle, the secondary use of health information is regarded as one of the most promising outcomes of the sharing of health data, even despite the existence of barriers (including quality problems with the data) which may slow implementation [33]. There are numerous possible data quality measures, including the use of a consistent patient identifier, the completeness of the data (measured for example, by the population coverage of electronic clinical records and key datasets) [34], data timeliness, and the level of granularity of the data. Population coverage can be monitored by establishing the proportion of health care organisations or professionals having access to electronic sharing and their viewing of shared data [35]. Granularity can be monitored by mapping the use of coding and classifications in stored and shared data [36].

The Nordic eHealth indicator work has highlighted the challenges as well as the opportunities of developing common performance indicators for information exchange and data sharing from the clinical perspective. Developing indicators to monitor access, quality, use, and value of shared data utilisation using Health Care Quality registers and data logs from national health information databases in addition to the survey data has been proposed as a next step in monitoring the safety and value of shared data utilisation [37].

5 Conclusion

The ongoing and dramatic developments in digital health are a big contributor to transformative changes across the health care system. Large data sharing endeavours can help to underpin new collaborative models of health care which provide *shared information, engagement, and accountability* across all stakeholders [38]. A robust commitment to evaluation is critical to delivering health data benefits and the establishment of collaborative models of health care well into the future. Some of the *key evaluation considerations* for ensuring the success of data governance frameworks and the realisation of health data benefits include: i) stakeholder consultation that ensures that stakeholders' views and values are adequately represented, e.g., by regularly monitoring usability and user satisfaction involved with (national) data sharing plans and implementations; ii) governance frameworks that are reviewed and renewed to reflect community values; and iii) the utilisation of current, best practice technologies, measures and methods to protect patient data privacy security and trustworthiness.

References

1. Andreu-Perez, J, Poon CC, Merrifield RD, Wong ST, Yang GZ, Big data for health. IEEE J Biomed Health Inform 2015;19(4): 1193-208.
2. Chen H, Chiang RH, Storey VC. Business intelligence and analytics: From big data to big impact. MIS Q 2012;36(4).
3. Bureau of Health Information. Data Matters - Linking data to unlock information. The use of linked data in healthcare performance assessment. Sydney, NSW: Bureau of Health Information; 2015.
4. Productivity Commission. Data Availability and Use: Overview and Recommendations. Report no 82. Canberra, Australia: Commonwealth of Australia; 2017.
5. Rigby M, Ronchi E. OECD-NSF Workshop: Building a Smarter Health and Wellness Future 15-16 February 2011. Summary Of Key Messages; Available on http://www.oecd.org/dataoecd/19/23/48915787.pdf, Accessed 20 November 2017. Paris: OECD.
6. Friedman C, Rigby M. Conceptualising and creating a global learning health system. Int J Med Inform 2013;82(4):e63-e71.
7. Coiera E. Guide to Health Informatics (Third Edition). Florida, USA: CRC Press; 2015.
8. Safran C, Bloomrosen M, Hammond WE, Labkoff

S, Markel-Fox S, Tang PC, et al. Toward a national framework for the secondary use of health data: an American Medical Informatics Association White Paper. J Am Med Inform Assoc 2007;14(1):1-9.
9. Gordon WJ, Fairhall A, Landman A. Threats to Information Security—Public Health Implications. New Engl J Med 2017;377(8):707-9.
10. Armstrong S. Data, data everywhere: the challenges of personalised medicine. BMJ 2017;359: j4546.
11. Rigby M, Georgiou A, Hyppönen H, Ammenwerth E, de Keizer N, Magrabi F, et al. Patient portals as a means of information and communication technology support to patient-centric care coordination - the missing evidence and the challenges of evaluation. Yearb Med Inform 2015;148-5.
12. Ammenwerth E. Evidence-based Health Informatics: How do we know what we know? Methods Inf Med 2015;54.
13. Sheikh A, Atun R, Bates DW. The need for independent evaluations of government-led health information technology initiatives. BMJ Qual Saf 2014;8:611-3.
14. Nykänen P, Brender J, Talmon J, Keizer N, Rigby M, Beuscart-Zephir M-C, et al. Guideline for good evaluation practice in health informatics (GEP-HI). Int J Med Inform 2011;80(12):815-27.
15. Talmon J, Ammenwerth E, Brender J, de Keizer N, Nykänen P, Rigby M. STARE-HI--Statement on reporting of evaluation studies in Health Informatics. Int J Med Inform 2009;78(1):1-9.
16. Scott P, Rigby M, Ammenwerth E, McNair JB, Georgiou A, Hyppönen H, et al. Evaluation Considerations for Secondary Uses of Clinical Data: Principles for an Evidence-based Approach to Policy and Implementation of Secondary Analysis. Yearb Med Inform 2017:59-67.
17. Kelly G, McKenzie B. Security, privacy, and confidentiality issues on the Internet. Jo Med Internet Res 2002;4(2).
18. Institute of Medicine. Beyond the HIPAA Privacy Rule: Enhancing Privancey, Improving Health Through Research. Washington DC, USA: The National Academies Press; 2009.
19. Organisation for Economic Co-operation and Development (OECD). New Health Technologies: Managing Access, Value and Sustainability. Paris, France: OECD Publishing; 2017.
20. Hordern A, Georgiou A, Whetton S, Prgomet M. Consumer eHealth - an overview of the research evidence and the implications for future policy. Health Inf Manag 2011;40(2):6-14.
21. Hemsley B, McCarthy S, Adams N, Georgiou A, Hill S, Balandin S. Legal, ethical, and rights issues in the adoption and use of the "My Health Record" by people with communication disability in Australia. J Intellect Dev Disabil 2017: 1-9.
22. Alston C, Berger ZD, Brownlee S, Elwyn G, Fowler JFJ, Kelly LK, et al. Shared Decision Making Strategies for Best Care: Patient Decision Aids. Discussion Paper. Available at: https://nam.edu/perspectives-2014-shared-decision-making-strategies-for-best-care-patient-decision-aids/. Accessed: 22 November 2017. 2014, Washington, DC.: Institute of Medicine.
23. Aicardi C, Del Savio L, Dove ES, Lucivero F, Tempini N, Prainsack B. Emerging ethical issues regarding digital health data. On the World Medical Association Draft Declaration on Ethical Considerations Regarding Health Databases and Biobanks. Croat Med J 2016;57(2): 207-13.
24. UK Department of Health Data Sharing and Cyber Security Team. Your Data: Better Security, Better Choice, Better Care. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/627493/Your_data_better_security_better_choice_better_care_government_response.pdf.Accessed: 28 October 2017. 2017.
25. Organisation for Economic Co-operation and Development. 2013 OECD Privacy Guidelines. Available at: www.oecd.org/internet/ieconomy/privacy-guidelines.htm. Accessed: 9 October 2017. 2013.
26. Global Observatory on eHealth. Third Global Survey on eHealth 2015. The use of eHealth in support of universal health coverage. World Health Organiziation; 2015.
27. Hyppönen H, Kangas M, Reponen J, Nohr C, Villumsen S, Koch S, et al. Nordic eHealth Benchmarking - Status 2014 (TemaNord; No. TemaNord 2015:539). Copenhagen; 2015.
28. Technology Informatics Guiding Education Reform (TIGER). The TIGER Nursing Informatics Competencies. Available: http://www.himss.org/ResourceLibrary/genResourceDetailPDF.aspx?ItemNumber=44660 (Accessed 21 November 2017). 2010.
29. Hyppönen H, Hahtela N, Suutarla A, Sillanpää K, Kinnunen U-M, Ahonen O, et al. Smart systems for capable users? Nurses' experiences on patient information systems 2017 (In Finnish, with English abstract) (In press). Finnish Journal of eHealth and eWelfare Finjehew (https://journal.fi/finjehew), 2018 (January).
30. Kaipio J, Lääveri T, Hyppönen H, Vainiomäki S, Reponen J, Kushniruk A, et al. Usability problems do not heal by themselves: National survey on physicians' experiences with EHRs in Finland. Int J Med Inform 2017;97:266-81.
31. Hyppönen H, Hyry J, Valta K, Ahlgren S. Electronic services in the social welfare and health care sector. Citizens' experiences and development needs Report 33/2014. Helsinki: National Institute for Health and Welfare (THL); 2014.
32. Hämäläinen P, Doupi P, Hyppönen H. eHealth policy and deployment in the European Union: Review and analysis of progress. Helskinki: Stakes; 2008.
33. Sandhu E, Weinstein S, McKethan A, Jain SH. Secondary uses of electronic health record data: benefits and barriers. Jt Comm J Qual Patient Saf 2012;38(1):34-40.
34. Hypponen H, Hamalainen P, Thonnet M, Nicholas L. Overview of OECD studies on eHealth and core outcome. Providing the first work on international activities outside EU. Available at: https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20161121_co31_en.pdf. Accessed 6 October 2017. 2016.
35. Organisation for Economic Co-operation and Development. OECD Guide to Measuring ICTs in the Health Sector. Available at: http://www.oecd.org/health/health-systems/Draft-oecd-guide-to-measuring-icts-in-the-health-sector.pdf. Accessed: 9 October 2017.
36. Vuokko R, Mäkelä-Bengs P, Hyppönen H, Lindqvist M, Doupi P. Impacts of structuring the electronic health record: Results of a systematic literature review from the perspective of secondary use of patient data. Int J Med Inform 2017;97:293-303.
37. Hypponen H, Koch S, Faxvaag A, Gilstad H, Nohr C, Hardardottir G, et al. Nordic eHealth benchmarking. TemaNord © Nordic Council of Ministers 2017. p. 528.
38. Millenson ML. When "patient centred" is no longer enough: the challenge of collaborative health. BMJ 2017;358:j3048.

Correspondence to:
Professor Andrew Georgiou
Centre for Health Systems and Safety Research
Australian Institute of Health Innovation
Macquarie University
6/75 Talavera Road
Macquarie University NSW 2109
Australia
Tel: +61 2 9850 2424
E-mail: andrew.georgiou@mq.edu.au