JOURNAL OF
INNOVATION IN
HEALTH INFORMATICS

Leading article

The UK National Data Guardian for health and care's review of data security, consent and opt-outs: leadership in balancing public health with rights to privacy?

Cite this article: Chan T, Di Iorio CT, Kuziemsky C, Liaw S-T, de Lusignan S, Lo Russo D. The UK National Data Guardian for health and care's review of data security, consent and opt-outs: leadership in balancing public health with rights to privacy? *J Innov Health Inform*. 2016;23(3):627–632.

http://dx.doi.org/10.14236/jhi.v23i3.909

Author address for correspondence:
Tom Chan
Section of Clinical Medicine and Ageing
Department of Clinical and Experimental Medicine
Faculty of Health and Medical Sciences
University of Surrey
Guildford, Surrey, UK
Email: t.chan@surrey.ac.uk

Accepted October 2016

Tom Chan
Section of Clinical Medicine and Ageing, Department of Clinical and Experimental Medicine, Faculty of Health and Medical Sciences University of Surrey, UK

Concetta Tania Di Iorio
Legal Consultant LL.M M.P.H, Serectrix s.n.c., Italy

Craig Kuziemsky
Telfer School of Management, University of Ottawa, Canada

Siaw-Teng Liaw
UNSW Medicine Australia, Ingham Institute of Applied Medical Research, Australia

Simon de Lusignan
Section of Clinical Medicine and Ageing, Department of Clinical and Experimental Medicine, Faculty of Health and Medical Sciences University of Surrey, Guildford, UK

Daniel Lo Russo
NHS Guildford & Waverley Clinical Commissioning Group (CCG), Guildford, UK

ABSTRACT

Sharing health and social care data is essential to the delivery of high-quality health care as well as disease surveillance and public health and for conducting research. However, these societal benefits may be constrained by privacy and data protection principles. Hence, societies are striving to find a balance between the two competing public interests. Whilst the spread of IT advancements in recent decades has increased the demand for an increased privacy and data protection in many ways, health is a special case.

The UK is adopting guidelines, codes of conduct and regulatory instruments aimed to implement privacy principles into practical settings and enhance public trust. Accordingly, in 2015, the UK National Data Guardian requested to conduct a further review of data protection, referred to as Caldicott 3. The scope of this review is to strengthen data security standards and confidentiality. It also proposes a consent system based on an 'opt-out' model rather than on 'opt-in'.

Across Europe as well as internationally, the privacy health data sharing balance is not fixed. In Europe, the enactment of the new EU Data Protection Regulation in 2016 constitutes a major breakthrough, which is likely to have a profound effect on European countries and beyond. In Australia and across North America, different ways are being sought to balance out these twin requirements of a modern society – to preserve privacy alongside affording high-quality health care for an ageing population.

Whilst in the UK privacy legal framework remains complex and fragmented into different layers of legislation, which may negatively impact on both the rights to privacy and health, the UK is at the forefront in the uptake of international and EU privacy and data protection principles. And, if the privacy regime was reorganised in a more comprehensive manner, it could be used as a sound implementation model for other countries.

INTRODUCTION

Sharing health and social care data is essential to the delivery of high-quality health care and health care monitoring.[1] Health information is also a valuable resource for surveillance of safety and evaluation of performance of the wider system of care services and for researches to improve treatments, care and outcomes at both the individual patient and the policy levels.[2]

However, the respect of privacy and data protection principles may pose legal constraints to the sharing of health information, even when it aims to societal benefits. As acknowledged in the literature, privacy is not an absolute right; hence, it should be weighed against other rights, including the right to health and health care. Hence, it is crucial that societies reach the best treadoff between the two competing interests and seek a right balance in the protection of both human rights.[3]

The increasing digitalisation of information in recent decades continuously has posed new challenges and threats to privacy and data protection. To this aim, the European Commission underwent a profound revision of the data protection regime[4] that brought to the enactment of the new Data Protection Regulation in April 2016. At the national level, several countries, including UK, are enacting regulations and code of conduct to address these new challenges and seek a balanced approach between privacy and health.

Public trust is also essential for allowing governments to collect and process reliable and high-quality information that would enhance public health and social care, and the assurance of health professionals is a crucial part of this.[5]

Ensuring that privacy and data security is guaranteed in data collection and processing, in a way that it acceptable to the public, is a key to improving health for all. This article describes the UK context and the leadership shown by its National Data Guardian (NDG), and then compares and contrasts this with European and other international examples.

THE UK MODEL OF PRIVACY PROTECTION AND ROLE OF THE NATIONAL DATA GUARDIAN

The Data Protection Act 1998[6] implemented the 1995 European Data Protection Directive. It provides the legal framework for the UK's data protection procedures. The Data Protection Act 1998 provided an exemption from the general prohibition of processing sensitive data for reasons of substantial public interests, which are specifically identified in statutory instruments. These general exemptions included data processing for research, historical and statistical purposes, subject to suitable safeguards.

Notwithstanding, the legal frameworks and national and professional guidance relating to data security and data sharing still remain complex in the UK. There had been a number of initiatives to summarise these guidance into a set of principles. One of the first and best know are the six Caldicott principles.[7] There has also been a code of practice on confidential information,[8] and a set of auditable standards for information security, the Information Governance Toolkit.[9]

Navigating the application processes to access data for research purposes can also be a daunting challenge and results in unwillingness to share data. A second Coldicott report[10] added a seventh principle that 'The duty to share information can be as important as the duty to protect patient confidentiality' to underline the importance of data sharing for legitimate purposes.

In September 2015, the Secretary of State for Health asked Dame Fiona Caldicott, NDG, to review systems of data security, consent and opt-outs. The report[11] of the review (also known as Caldicott 3) was published in June this year.

Whilst general UK citizens trust the NHS to protect confidentiality of information, there have been cases where breaches of security or inappropriate sharing of confidential information occurred, eroding this trust. In response, the UK government updated the NHS Constitution in 2013[12] and introduced a new right for patients to request that their information is not shared beyond their own care and requested specific items of information not to be shared with others involved in providing their care.

Box 1 UK National Data Guardian – Consent/Opt-out model

- Patients' confidentiality is a principle protected by law
- Health data and information are essential for high quality care,
- Information is needed to improve the safety and quality of care through
    - o Research
    - o Service/system evaluation
    - o Protection of public health
- Endorses existing right that patients may, at any time, opt out from their confidential information being shared beyond their own care as guarantee by the NHS Constitution
- The possibility of opting-out is waived where
    - o Mandatory legal requirement or
    - o Overriding public interest including
        - ▪ Notifiable diseases
        - ▪ Child or vulnerable adult safety purposes
- Consultation on whether the opt-out choice could be in two parts:
    1. Opt-out where data are processed for use in NHS and social care system
    2. Opt-out model for data processed for research

UK National Data Guardian report – leadership and trust

The first sentence of the NDG's review report read: 'This is a report about trust'. The report seeks to underpin trust in two ways: (1) Ensuring the security of health and social care data and (2) That implied consent combined with an option to opt out from data sharing.

The report called for two local leadership roles: (1) Senior Information Risk Owner (SIRO) – a senior manager who

takes ownership of the organisation's information risk policy) and (2) Caldicott Guardian – a senior clinician responsible for protecting the confidentiality of patient information and enabling appropriate information sharing.

It describes the leadership obligations in the three 'pillars' of information security: (1) people, (2) process and (3) technology (Box 2), underpinned by ten detailed data security standards.

In summary, the UK model is one of National legislation and standards with citizen opt-outs; with the NDG trying to pull these elements together to create a technically secure and trusted environment.

Box 2 UK National Data Guardian (NDG) – The obligations of leaders - the three pillars

1. **People: Ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles**
   The standards within this 'pillar' include that all staff will complete appropriate annual security training and pass a mandatory test
2. **Process: Ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses**
   The standards within this 'pillar' include: -
   - Confidential data are accessible only to staff who need it for their current role and access is removed as soon as it is no longer required
   - Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses
   - Cyber-attacks are identified and resisted and security advice is responded to;
   - Continuity plans are in place to respond to threats to data security
3. **Technology: Ensure technology is secure and up-to-date**
   The standards within this 'pillar' include
   - No unsupported operating systems, software are used; a strategy is in place to respond to threats to data security
   - IT suppliers are held accountable via contracts for protecting confidential data

The evolution of Privacy and Data Protection at International and EU levels

Many international instruments recognized privacy as a fundamental human right:

- 1948 Universal Declaration of Human Rights[13]
- International Covenant on Civil and Political Rights (ICCPR)[14]
- UN Convention on Migrant Workers[15]
- UN Convention on Protection of the Child.[16]

In Europe, the right to privacy was legally enforced by the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms[17]; it states:

'Everyone has the right to respect for his private and family life, his home and his correspondence'. The Convention created the European Commission of Human Rights and the European Court of Human Rights to oversee enforcement.

In the development of privacy protection, the Council of Europe's 'Convention for the protection of individuals with regard to the automatic processing of personal data'[18] and the Organization for Economic Cooperation and Development's 'guidelines governing the protection of privacy and transborder data flows of personal data'[19] profoundly influenced the enactment of laws around the world during the 60s and 70s.

The 1995 Data Protection Directive[20] includes provisions about the processing of health data. Article 8(3) relaxes the provision of the directive for preventive medicine, medical diagnosis, the provision that restricts the processing of health data where it is for care or treatment and the management of health care services, where data are processed by a health professional subject under national law. Also, Member States may, under Article 8(4), for reasons of substantial public interest, lay down additional exemptions.

The Council of Europe Convention on Human rights and Biomedicine (Oviedo 1997) reinforced the principles that everyone is entitled to the right to privacy and confidentiality of personal medical data and the right to be informed about his/her health.[21]

The Charter of Fundamental Rights, entered into force on 1 December 2009 as part of the Treaty of Lisbon,[22] provided the Union of its own catalogue of rights including:

'Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority'.

The New EU Data Protection Regulation (2016)

The spread of new technological developments alongside the need to make data available to enable the effective delivery of health and social care have both influenced the new EU Regulations.

Generally, they strengthen individuals' rights – consent is needed for their data to be processed and similarly they have the right to be forgotten. It also introduces tougher penalties for breeches in security. However, the Regulation also specifically acknowledges pseudonymisation as a privacy protection measures (Box 3).

Box 3 Definition of pseudonymisation – from http://www.epsos.eu/faq-glossary/glossary.html

Pseudonymisation is the process of disguising patient identity. In contrast to fully anonimized data, pseudonymisation allows future or additional data to be linked to the current data, whereby the identity of the patient remains undisclosed.

The processing of personal health data can occur without consent 'For reasons of public interest in the areas of public health' if it is based on the union or member state law. 'Public health' is given a very broad definition: 'All elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality'. This reasonably extends to health research, statistics, monitoring, health system performance and governance. Additionally, data do not have to only be held by health professionals.

States must 'establish specifications for determining the controller, the type of personal data that are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing'.

These regulations pave the way for initiatives such as those of the UK's NDG.

Canada has an overarching Federal act, the Personal Information Protection and Electronic Documents Act (PIPEDA), which governs how private sector organizations collect, use or disclose personal information, including health care data[23]. PIPEDA is supplemented by public and, in some cases, private sector legislations, in each individual province or territory; some of which directly pertain to health care data (e.g. the *Personal Health Information Protection Act* in Ontario).

The United States has laws specific to individual sectors with the Health Insurance Accountability and Portability Act[24] and the Health Information Technology for Economic and Clinical Health Act[25] are the two primary federal acts responsible for protecting personal health care information. Both Canada and the USA struggle with finding the balance between protecting individual data and advancing the greater societal good such as health research and surveillance.[26] The consent model for research and purposes other than the reason for data collection is opt out in both Canada and the USA, although certain public health and surveillance activities are granted exceptions.[27]

International approaches to balancing privacy and health needs[2] – Australia

The Australian Privacy Act 1988 'governs' the National Information Privacy Principles,[28] which forms the 'soft law' that guides the implementation of the elements of the privacy act. The Australian information privacy commissioner has the authority to use and disclose information to appropriate authorities as part of any investigations into alleged contraventions of this and the Personally Controlled Electronic Health Record (PCEHR) Act.

The PCEHR is now called 'MyHealthRecord (MHR)'. Consent to disclose or use health information from MHR may be waived if there is a serious threat to the safety of the consumer or public, or for law enforcement through a court or tribunal. Participants in the MHR system must not hold or take the records outside Australia if it includes personal and identifying information relating to the consumer and participants in the MHR system.

The MHR system has been poorly adopted by heath care providers and patients alike.[29] Reasons include the 'opt-in' consent model and poor clinician engagement to ensure usability. The current trials on the 'opt-out' consent model in designated areas in Australia are due to report soon, which may provide clarity on the safe use and disclosure of MHR information.

It is left to local initiatives to try to link well-defined geographical neighbourhood to provide insights into clinical indicators and health services use in the context of integrated care.[30] Much more needs to be done around the custodianship and stewardship of repositories of EHR data.[31]

Australia appears to be struggling with low uptake of an opt-in model.

DISCUSSION

The UK NDG's recent initiative sets out how more stringent security, local leadership, and a more developed opt-out model could potentially improve patient and public trust in data sharing.

This approach is compatible with the New EU Regulations. They are a major breakthrough in the development of privacy and data protection in European countries by allowing member states, for the first time, to establish a coherent privacy and data protection legal framework for the health sector, including health research, within the framework of EU Regulation. These regulations accept the need for using approaches like pseudonymisation that data need to be used for health system management and that this needs to encompass health and social care.

The UK NDG also provides an approach compatible with that being developed across North America. The recommendations in the NDG's report could contribute to the design of policy for governance of personal health care information in Canada and the United States, as they both struggle with the balance between protection of individual data and the growing need for research to support the common good. In Canada, navigating the current system of federal and provincial privacy legislation can be a substantial barrier to health system research and health system improvement, accordingly. The NDG's approach is somewhat at odds with the Australian approach of launching an online opt-in system. Attempts to advance this type of approach in both England and France have failed.[32]

A harmonized and balanced approach to privacy and data protection, valued against compelling societal interests and rights such as the right to health and health and social care, seems to be missing. The UK's NDG may be pointing towards an approach to bridge that gap – but the approach may not be readily generalisable.

CONCLUSION

The EU Data Protection Regulation 2016 constitutes a comprehensive legal framework for European countries. However, the way it will be implemented in national settings will surely

impact on the level of harmonization across Europe, which still remains uncertain.

UK has already implemented most of the EU privacy and data protection principles contained in the new Regulation. However, the lack of a general and comprehensive legal framework for the health and social care sectors causes some uncertainties on how to handle health data in practical settings. The UK would benefit of a reorganization of the privacy regime that would move towards the definition of a harmonized discipline of privacy and data protection in the health and social care sectors.

The UK, with its NDG, and local SIRO and Caldicott guardians may well be at the forefront in the uptake of privacy and data protection principles, and if the privacy regime were reorganized in a more comprehensive manner across health and social care, it could be used as a sound implementation model for many other countries.

REFERENCES

1. de Lusignan S, Liyanage H, Di Iorio CT, Chan T and Liaw S-T. Using routinely collected health data for surveillance, quality improvement and research: Framework and key questions to assess ethics, privacy and data access. *Journal of Innovation in Health Informatics* 2015;22(4):426–432. http://dx.doi.org/10.14236/jhi.v22i4.845.
2. de Lusignan S and van Weel C. The use of routinely collected computer data for research in primary care: opportunities and challenges. *Family Practice*. 2006;23(2):253–63. http://dx.doi.org/10.1093/fampra/cmi106. PMid:16368704.
3. Di Iorio CT, Carinci F and Oderkirk J. Health research and systems' governance are at risk: should the right to data protection override health? *Journal of Medical Ethics* 2014;40(7):488–92.
4. Carinci F, Di Iorio CT, Ricciardi W, Klazinga N and Verschuuren M. Revision of the European Data Protection Directive: opportunity or threat for public health monitoring? *European Journal of Public Health* 2011;21(6):684–7. http://eurpub.oxfordjournals.org/content/21/6/684.long. http://dx.doi.org/10.1093/eurpub/ckr100. PMid:21785116.
5. de Lusignan S, Chan T, Theadom A and Dhoul N. The roles of policy and professionalism in the protection of processed clinical data: a literature review. *International Journal of Medical Informatics* 2007;76(4):261–8. http://dx.doi.org/10.1016/j.ijmedinf.2005.11.003. PMid:16406791.
6. UK Data Protection Act 1998. http://www.legislation.gov.uk/ukpga/1998/29/contents.
7. The Caldicott Committee. Report on the Review of Patient-Identifiable Information. Department of Health, Dec 1997.
8. Health and Social Care Information Centre. Code of practice on confidential information. 2014. Available from: http://systems.digital.nhs.uk/infogov/codes/cop/code.pdf. Accessed August 22 2016.
9. Department of Health. Information Governance Toolkit. Available from: https://www.igt.hscic.gov.uk/.
10. Department of Health. To Share or Not to Share? Information Governance Review. Department of Health. 2013 Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf.
11. National Data Guardian for Health and Care's Review of Data Security, Consent and Opt-Outs. 2016. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF.
12. Department of Health. The NHS Constitution: the NHS belongs to us all. 2012. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/480482/NHS_Constitution_WEB.pdf.
13. Universal Declaration of Human Rights, adopted and proclaimed by General Assembly Resolution 217 A (III). 1948. Available from: http://www.un.org/Overview/rights.html.
14. International Covenant on Civil and Political Rights, adopted and opened for signature, ratification and accession by General Assembly Resolution 2200A (XXI). 1966. Available from: http://www.unhchr.ch/html/menu3/b/a_ccpr.htm.
15. International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, adopted by General Assembly Resolution 45/158. 1990. Available from: http://www.unhchr.ch/html/menu3/b/m_mwctoc.htm.
16. Convention on the Rights of the Child, adopted and opened for signature, ratification and accession by General Assembly Resolution 44/25. 1989. Available from: http://www.unhchr.ch/html/menu3/b/k2crc.htm.
17. Council of Europe. *Convention for the Protection of Human Rights and Fundamental Freedoms (ETS no: 005)*. Strasbourg: The Council, 1950. Available from: http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm.
18. Council of Europe. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.* Strasbourg: The Council, 1981. Available from: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.
19. OECD. *Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data*. Paris: OECD, 1981. Available from: http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM.
20. OJEC. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on The Free Movement of Such Data.* Official Journal of the European Communities No. L 281/31. Luxembourg: Official Journal of the European Union, 1995. Available from: http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm.
21. Committee of Legal Advisers on Public International Law. *Council of Europe Convention on Human Rights and Biomedicine.* Oviedo: Committee of Legal Advisers on Public International Law, 1997. Available from: http://conventions.coe.int/Treaty/EN/Treaties/Html/164.htm.
22. OJEC. *Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, Signed at Lisbon, 13 December 2007*. Luxembourg: Official Journal of the European Union. 2007/C 306/01. Available from: http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2007:306:SOM:EN:HTML.
23. Office of the Privacy Commissioner of Canada. Overview of privacy legislation in Canada. Available from: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/.
24. The U.S. Department of Health and Human Services. The Health Insurance Portability and Accountability Act. Available from: http://www.hhs.gov/hipaa/. Accessed 4 October 2016.
25. SearchHealthIT. Health Information Technology for Economic and Clinical Health Act. Available from: http://searchhealthit.techtarget.com/definition/HITECH-Act. Accessed on 4 October 2016.
26. Liyanage H. et al. Building a privacy and ethics framework for real world/computerised medical record system data: A Delphi study. Primary Health Care Informatics Working Group contribution to the Year Book of Medical Informatics 2016 (in press).

27. Birnbaum D, Borycki E, Karras BT, Denham E and Lacroix P. Addressing public health informatics patient privacy concerns. *Clinical Governance* 2015;20(2):91–100. http://dx.doi.org/10.1108/CGIJ-05-2015-0013.
28. Office of the Australian Information Commissioner. The Australian Privacy Act 1988. Sydney: OAIC, 1988. Available from:https://www.oaic.gov.au/privacy-law/privacy-archive/privacy-resources-archive/information-privacy-principles.
29. The Australian Government. Available from: https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/Content/news-002.
30. Liaw ST and de Lusignan S. An integrated health neighbourhood framework to optimise the use of EHR data. *Journal of Innovation in Health Informatics* 2016; 23(3): 547–554 http://dx.doi.org/10.14236/jhi.v23i3.826.
31. Liaw ST, Powell-Davies G, Pearce C, Britt H, McGlynn L and Harris MF. Optimising the use of observational EHR data: current issues, evolving opportunities, strategies and scope for collaboration. *Australian Family Physician* 2016; 45(3):153–156. PMid:27052055.
32. de Lusignan S and Seroussi B. A comparison of English and French approaches to providing patients access to Summary Care Records: scope, consent, cost. S*tudies in Health Technology and Informatics* 2013;186:61–5. PMid:23542968.