JOURNAL OF INNOVATION IN HEALTH INFORMATICS

Leading article

Using routinely collected health data for surveillance, quality improvement and research: Framework and key questions to assess ethics and privacy and enable data access

Simon de Lusignan
Department of Clinical and Experimental Medicine, University of Surrey, UK

Harshana Liyanage
Department of Clinical and Experimental Medicine, University of Surrey, UK

Concetta Tania Di Iorio
Serectrix snc, Pescara, Italy

Tom Chan
Department of Clinical and Experimental Medicine, University of Surrey, UK

Siaw-Teng Liaw
School of Public Health and Community Medicine, UNSW Medicine, Australia

Cite this article: de Lusignan S, Liyanage H, Di Iorio CT, Chan T, Liaw S-T. Using routinely collected health data for surveillance, quality improvement and research: Framework and key questions to assess ethics and privacy and enable data access. *J Innov Health Inform*. 2015;22(4):426–432.

http://dx.doi.org/10.14236/jhi.v22i4.845

Author address for correspondence:
Simon de Lusignan
Department of Clinical and Experimental Medicine
University of Surrey
Guildford
Surrey GU2 7XH, UK
Email: s.lusignan@surrey.ac.uk

Accepted December 2015

ABSTRACT

Background The use of health data for public health, surveillance, quality improvement and research is crucial to improve health systems and health care. However, bodies responsible for privacy and ethics often limit access to routinely collected health data. Ethical approvals, issues around protecting privacy and data access are often dealt with by different layers of regulations, making approval processes appear disjointed.

Objective To create a comprehensive framework for defining the ethical and privacy status of a project and for providing guidance on data access.

Method The framework comprises principles and related questions. The core of the framework will be built using standard terminology definitions such as ethics-related controlled vocabularies and regional directives. It is built in this way to reduce ambiguity between different definitions. The framework is extensible: principles can be retired or added to, as can their related questions. Responses to these questions should allow data processors to define ethical issues, privacy risk and other unintended consequences.

Results The framework contains three steps: (1) identifying possible ethical and privacy principles relevant to the project; (2) providing ethics and privacy guidance questions that inform the type of approval needed; and (3) assessing case-specific ethics and privacy issues. The outputs from this process should inform whether the balance between public interests and privacy breach and any ethical considerations are tipped in favour of societal benefits. If they are then this should be the basis on which data access is permitted. Tightly linking ethical principles to governance and data access may help maintain public trust.

Keywords: confidentiality, jurisprudence, patient data privacy, patient rights, public health surveillance, research ethics

INTRODUCTION

Health research projects conducted in an international setting are increasingly attempting to bring together large data sets utilising patient's computerised medical record data.[1] Advances in secure computational methods make projects of this nature feasible and able to meet strict information governance standards that reduce the chances of any breach in privacy.

Privacy and ethical issues in real-life projects are complex and often project specific. Variations in published guidelines are influenced by the type of study participants, funding bodies, regional legislation, and so on.[2] Despite these differences, privacy and ethics are fundamental principles in biomedical science. The privacy and ethical framework described in this paper provides a generic evidence-based approach, with a focus on linking principles to practical questions that inform the approvals required to enable health data access. It recognises that research must be in the public interest and have citizens' trust.[3,4]

NEED FOR A PRAGMATIC APPROACH FOR DEALING WITH PRIVACY AND ETHICAL ISSUES

Many projects deal with ethical, privacy and data access issues within the same work package or committee. However, while they might be grouped together at the project-level, ethical approvals (if any) required for surveillance, quality improvement (QI) and research projects are subject to layers of regulation different from those that ensure privacy standards. Approvals are generally made by separate bodies that deal with specific areas. In general research ethics approval, or exemption from it, is dealt with separately from data protection and information governance. Moreover, approvals for international studies are obtained from separate bodies in different countries. This paper proposes a pragmatic methodology for researchers who want to use health care data for research, surveillance and service evaluation projects spanning from a conceptual framework to actionable assessment techniques.

BUILDING A PRIVACY AND ETHICAL FRAMEWORK

The privacy and ethical framework consists of a set of privacy and ethical assessment principles derived by a review of the relevant ethics and privacy literature (Table 1). The associated questions were developed by translating principles to fit the context of the potential use cases that the principles will be applied to. We considered examples in the existing literature that highlighted implications of applying (or not applying) privacy and ethical principles within specific health research settings or scenarios.

The framework adopts controlled vocabularies and standard definitions to ensure consistent understanding of the privacy and ethical principles. The set of principles and questions are extensible and can evolve in a manner that can absorb new research in the area and to adapt to changing legislations. The principles and questions are referenced to their original source.

Table 1 Key information sources

	First Author	Year	Brief title	Contribution	Step of framework
1	Beauchamp	1994	Methods and principles in biomedical ethics	Text book with an emphasis on the four core ethical principles (respect for autonomy, non-maleficence, beneficence and justice)	Ethical principles
2	Thompson	2006	Pandemic influenza preparedness: an ethical framework to guide decision making	Proposed a framework including 10 ethical values in the context of influenza epidemics.	Ethical principles
3	Tangwa	2009	Ethical principles in health research and review process	Reports ethical principles and related case studies	Ethical principles
4	Malin	2011	Identifiability in biobanks: models, measures and mitigation strategies	Discusses several key privacy characteristics specifically focusing on identifiability.	Privacy principles
5	Faden	2013	An ethical framework for a learning health care system	Describes an ethical framework with 7 ethical obligations in learning health care systems.	Ethical principles
6	Di Iorio	2013	Cross-border flow of health information: is 'privacy by design' enough?	Proposes a privacy assessment framework with 11 privacy factors.	Privacy principles
7	Babu	2014	An appraisal of the tuberculosis programme in India using an ethical framework	Summarises a set of 5 ethical issues associated to public health initiatives.	Ethical principles
8	Willison	2014	What makes public health studies ethical?	Provides ethical guiding questions for public health studies	Ethical guidance questions
9	O.E.C.D	2015	Health data governance: privacy, monitoring and research	Provides key health data governance mechanisms to maximise privacy risks and societal benefits	Data governance and privacy guidelines

CONTROLLED VOCABULARIES FOR REPRESENTING PRIVACY AND ETHICS

Controlled vocabularies are important to ensure consistency of the concepts used across studies and in different countries.[5] This approach is needed because the terminologies used for describing privacy, ethics and data access concepts are diverse. For example, the definitions of terms such as 'data owner', 'data custodian' and 'data processor' have overlapping meanings. Legal definitions, in the field of data protection, are often used very differently from how the same terms are used in research projects. We have built on a prior initiative for developing controlled vocabularies and ontologies in this domain.[6] We have extended this work by enriching the controlled vocabularies with additional findings from our literature survey and by adopting standard definitions accepted within the domain (e.g. European Union Data Protection Directive,[7] or other regionally appropriate definitions such as the Australian Privacy Principles[8]).

Step 1: Exploring ethical and privacy principles

The first step is to consider key (1) ethical and (2) privacy principles relevant to the research being conducted. Areas are included, or not, depending on the nature of the study.[1,9–16]

Step 2: Ethical and privacy questions to inform the approvals needed

The second stage involves asking and answering the ethical and privacy guidance questions for the principles that apply to that study. The guidance questions will be grounded on the identified ethical principles. They will support privacy and ethical evaluation of research studies and issues that arise during the lifetime of the projects. Researchers should include privacy and ethical considerations relevant to their study design and through this process identify what approvals are needed.[17] Data custodians can also use these questions to assess requests to share data.

Step 3: Should access to data be granted?

The responses to questions in Step 2 should inform whether there is an ethical basis for data access. Key areas to consider are: (1) mitigation strategies to be implemented to conform to privacy and ethical principles; (2) data flow modifications, that is any change in data processing to enhance privacy (e.g. use of aggregated data rather than with identifiable personal information); (3) what local approvals need to be put in place, which may be nationally stipulated and (4) protocols for data access; the use of pooled data may be authorised; alternatively, distributed analysis or a hybrid.

Ethical principles	Privacy principles
1) Autonomy	1) Accountability of personal information
2) Respect rights and dignity of patients	2) Collection of personal information
3) Respect clinical judgment of clinician	3) Consent
4) Duty to Provide Care	4) Use of personal information
5) Protection of the public from harm	5) Disclosure and disposition of personal information
6) Beneficence	6) Accuracy of personal information
7) Justice	7) Safeguarding personal information
8) Non-maleficence (an obligation not to inflict harm intentionally)	8) Openness/transparency
9) Reciprocity	9) Individual access to personal information
10) Solidarity	10) Challenging compliance to ensure accountability is achievable
11) Stewardship	11) Anonymisation process for secondary uses of health data
12) Trust	12) Lawfulness
13) Lawfulness	13) De-identification process
14) Transparent project approval process	14) Data linkage

USE CASES

The framework can be represented as a number of use cases involving multiple stakeholders; they will vary according to the type of study. The overall use case diagram for the framework is illustrated in Figure 1. 'Use cases' are generally used to model systems and their interactions in software engineering. They describe a story of how a system and its actors (those who engage in various interactions with the system) collaborate to achieve a specific goal. These diagrams are frequently used while gathering technical requirements associated with health information systems.[18,19] We have followed Unified Modelling Language use case notation as given in the Rational Unified Process to create these diagrams.[20]

1. Researchers and research ethics committees: The same principles and questions should apply to all involved in research. Privacy and ethics are included in the design of a study, and generally studies go on to receive ethical approval as the potential issues are considered from the initial stages. The actors in this use case will typically involve primary investigators who design the study, the ethics committee members who approve studies and data custodians who provide approval for data access. The ethics of research studies will have a higher degree of scrutiny as interventions might include new treatments.
2. QI: A narrower range of privacy and ethical considerations generally apply to QI initiatives. Protection of public from harm is generally not an issue

as most parts of those studies usually have a high degree of patient safety in built. Treatment used in QI studies are already approved and whether to treat is decided by both the clinician and the patient according to clinical standards and patient's preference. As data are generally handled at a local level, data sharing is less complicated in this use case.

3. Surveillance: Generally, using data for disease surveillance is part of a health system's public health functions and therefore fewer ethical principles apply. However, a duty of privacy remains where data are further used to inform QI or research; in which case different principles pertain. Data are mostly reported as aggregated summaries and the unit used for reporting is generally regional or city level though sentinel surveillance networks report at the national level. The unit of reporting largely ensures that privacy of individuals is maintained despite reports are published at regular intervals. However, privacy concerns might arise when stratifying populations into narrow age-bands or localities and in the reporting of rare events. During epidemic outbreaks, personal data and samples may need to be collected for public health purposes. Whilst the privacy and ethical considerations applied in this use case are limited, patients should still be given the right to opt out of their data being used for surveillance.

The use cases also involve representatives from the public including patients, carers (generally parents in the case of children) and non-patient citizens. Present-day research studies should have a high level of patient and public engagement throughout the research process. Patient group representatives should get involved as early as the design stage of the study to ensure that studies are likely to be beneficial to patients and to help maintain wider public trust. We have drawn secondary-level use cases suggesting how the privacy and ethical framework will be utilised (Figures 2–4).

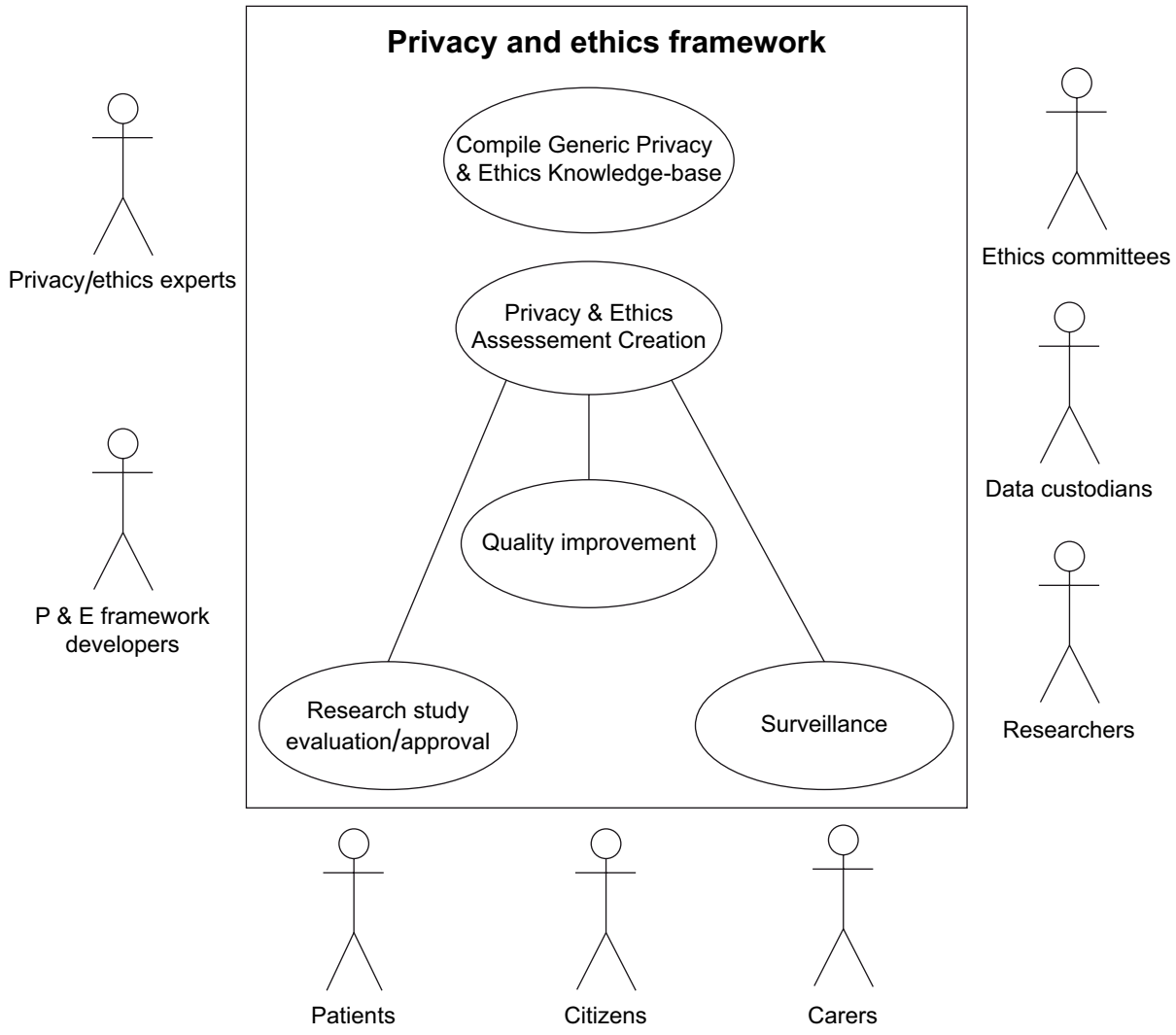

Figure 1 Overall use case diagram for the privacy and ethical framework. The box indicates the system of interest and the oval within corresponds to the processes within the system that are inter-related. The actors who interact with the system (and its processes) are drawn around the box

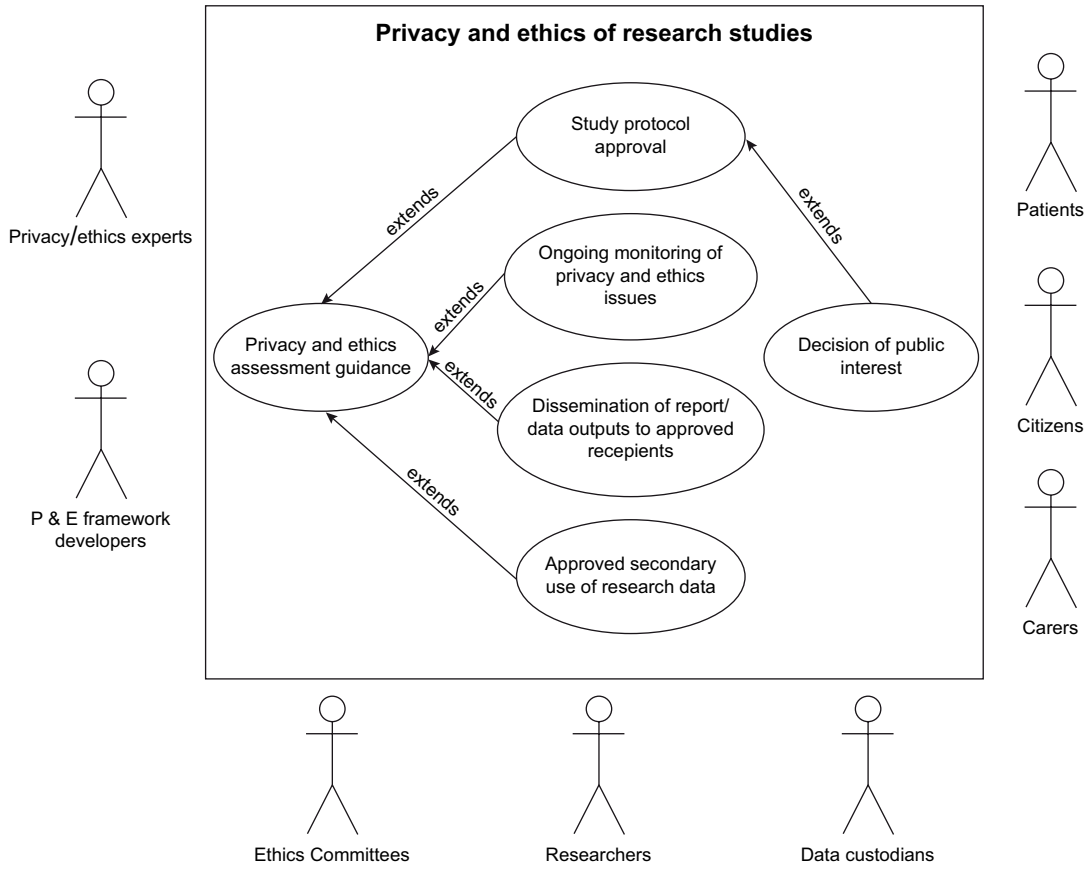

Figure 2 **The use case utilising the privacy and ethics framework in the context of research studies. Research requires the greatest level of scrutiny and involvement of actors – eight different actors are identified as important in this process. Citizens are important as research in the public interest must also be acceptable to citizens. Patients include consenting research participants and carers include parents and those with power of attorney**

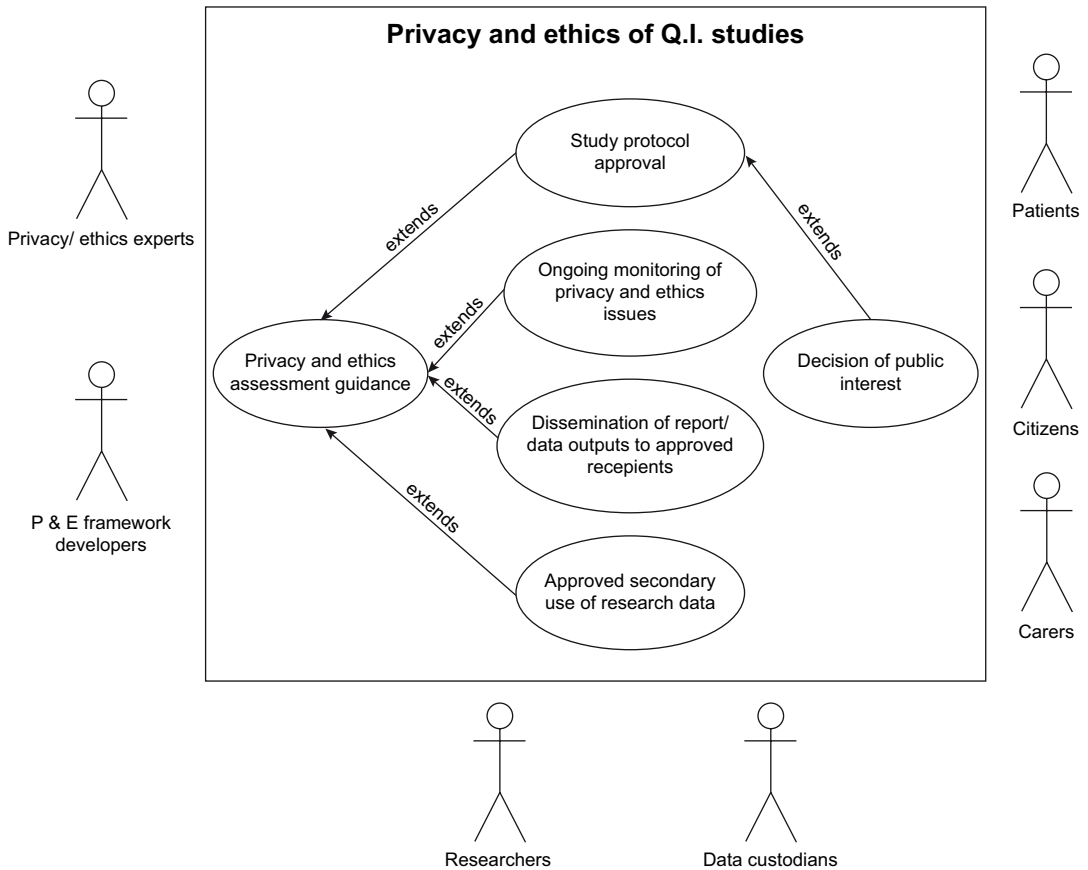

Figure 3 **The use case for utilising the privacy and ethics framework for QI studies. Generally, ethical approval is not required here in contrast to the research use case. Public interest is also important in this use case. QI studies requires a protocol just as research studies**

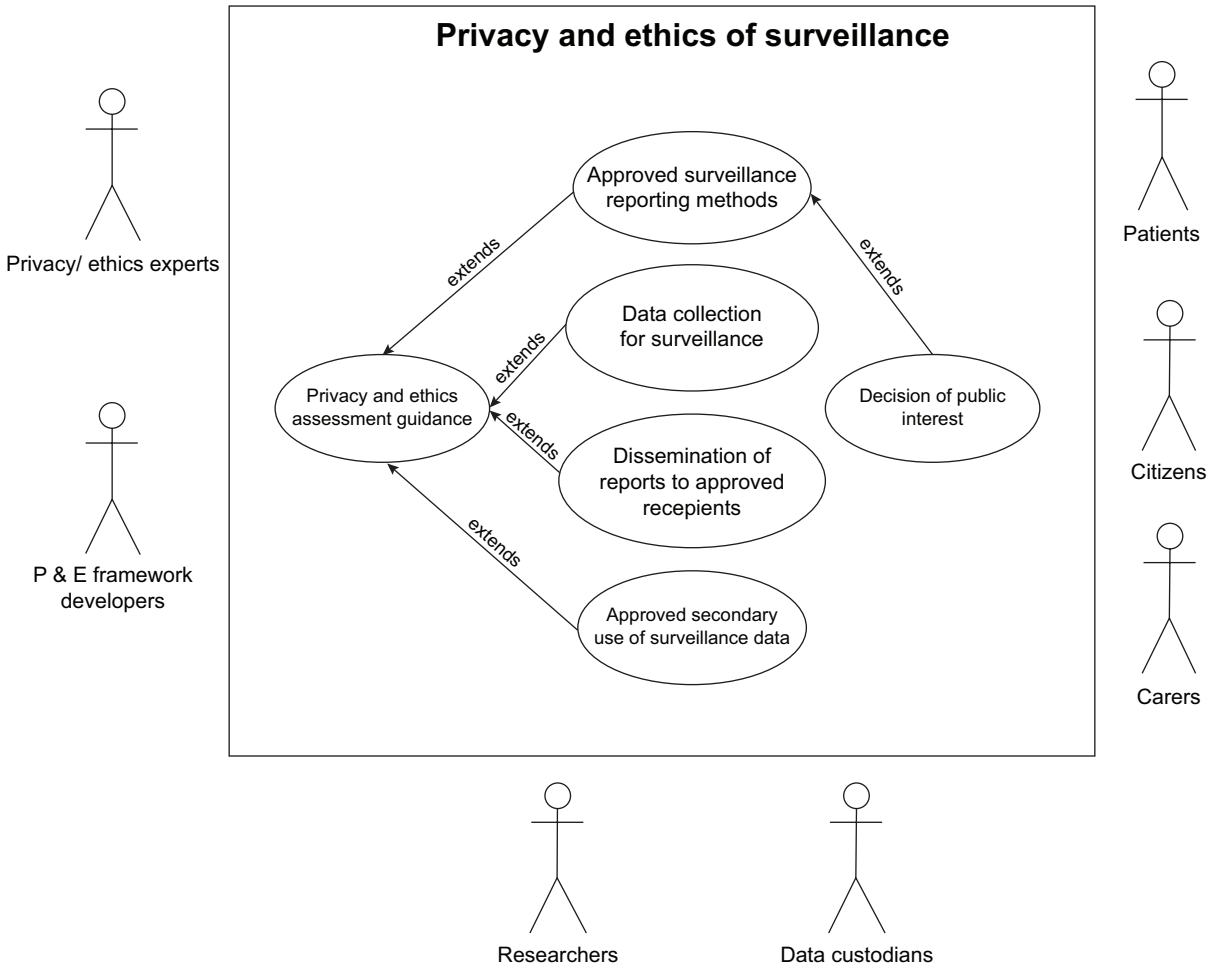

Figure 4 The use case for utilising the privacy and ethics framework for surveillance. Surveillance is conducted in the public interest, and although it does require clear reporting methods, it does not require a protocol or research ethical approval. However, individuals still have the right to expect that their privacy is protected. Only for a small number of specified diseases is legal compulsory information passed to public health specialists (e.g. Salmonella food poisoning)

SUMMARY

This paper describes an extensible framework that can be used to explore the ethical and privacy principles related to research, QI and surveillance. The framework links to key questions that help ensure that important issues are identified. Further research is needed to test the reliability of this approach and the completeness and validity of the principles included in it. This is planned as an activity of the International Medical Informatics Association and European Federation for Medical Informatics Primary Health Care Working Groups.

The strength of this approach is the extensibility and adaptability to different research scenarios, as demonstrated in the example use cases. The coupling of ethical principles with the privacy and data protection requirements to access data represents a change from current practice, where they are often considered separately. The purpose of this integration is to help maintain the trust of citizens by ensuring that the use of routine health data is for ethical purposes and demonstrably in the public interest.

REFERENCES

1. OECD, *Health Data Governance: Privacy, Monitoring and Research, OECD Health Policy Studies*, Paris: OECD Publishing, 2015. Available from http://dx.doi.org/10.1787/9789264244566-en. Accessed on 20 Nov 2015.
2. Liaw ST and Tam CW. Research ethics and approval process: a guide for new GP researchers. *Australian Family Physician* 2015;44(6):419–22.
3. 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.
4. Cayton H and Denegri S. Is what's mine my own? *Journal of Health Services Research and Policy* 2003;8(Suppl 1):33–5.
5. Liyanage H, Krause P and de Lusignan S. Using ontologies to improve semantic interoperability in health data. *Journal of Innovation in Health Informatics* 2015;22(2):309–15.
6. Koepsell D, Arp R, Fostel J and Smith B. Creating a Controlled Vocabulary for the Ethics of Human Research: Towards a

Biomedical Ethics Ontology. *Journal of Empirical Research on Human Research Ethics* 2009;4(1):43–58. http://dx. doi:10.1525/jer.2009.4.1.43.

7. European Union. EU Directive 95/46/EC – The Data Protection Directive. Available from http:// www.dataprotection.ie/docs/EU-Directive-95-46-EC--Chapter-2/93.htm. Accessed on 20 Nov 2015.
8. Australian Privacy Principles. Available from https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles. Accessed on 20 Nov 2015.
9. Malin B, Loukides G, Benitez K and Clayton EW. Identifiability in biobanks: models, measures and mitigation strategies. *Human Genetics and Embryology* 2011;130(3):383–92.
10. Di Iorio CT, Carinci F, Brillante M, Azzopardi J, Beck P and Bratina N et al. Cross-border flow of health information: is 'privacy by design' enough? Privacy performance assessment in EUBIROD. *European Journal of Public Health* 2013;23(2):247–53.
11. Faden RR, Kass NE, Goodman SN, Pronovost P and Tunis S et al. An ethics framework for a learning health care system: a departure from traditional research ethics and clinical ethics. *The Hastings Center Report* 2013;S16–27.
12. Babu GR, Tn S, Bhan A, Lakshmi JK and Kishore M. An appraisal of the tuberculosis programme in India using an ethics framework. *Indian Journal of Medical Ethics* 2014;11(1):11–5.
13. Willison DJ, Ondrusek N, Dawson A, Emerson C, Ferris LE and Saginur R et al. What makes public health studies ethical? Dissolving the boundary between research and practice. *BMC Medical Ethics* 2014;15:61.
14. Tangwa GB. Ethical principles in health research and review process. *Acta Tropica* 2009;112(Suppl 1):S2–7.
15. T.L. Beauchamp and J.F. Childress. *Principles of Biomedical Ethics*, fourth edition. New York: Basic Books, 1994.
16. Thompson AK, Faith K, Gibson JL and Upshur RE. Pandemic influenza preparedness: an ethical framework to guide decision-making. *BMC Medical Ethics* 2006;7:E12.
17. Lowrance W. Learning from experience: privacy and the secondary use of data in health research. *Journal of Health Services Research and Policy* 2003 Jul;8 (Suppl 1):2–7.
18. de Lusignan S, Cashman J, Poh N, Michalakidis G, Mason A and Desombre T et al. Conducting requirements analyses for research using routinely collected health data: a model driven approach. *Studies in Health Technology and Informatics* 2012;180:1105–7.
19. Kuchinke W, Ohmann C, Verheij RA, van Veen EB, Arvanitis TN and Taweel A et al. A standardised graphic method for describing data privacy frameworks in primary care research using a flexible zone model. *International Journal of Medical Informatics* 2014;83(12):941–57.
20. Jacobson I, Grady B and James R. *The unified Software Development Process*. Boston: Addison-Wesley, 1999;1.

APPENDIX A – ETHICAL GUIDANCE QUESTIONS

Adapted from Willison et al. (2014)

1. What are the burdens and potential harms associated with the proposed initiative? Who bears them?
2. Are burdens and potential harms justified in light of the potential benefits to participants and/or to society?
3. Is the selection of participants fair and appropriate?
4. Is individual informed consent warranted? Is it feasible? Is it appropriate? Is it sufficient?
5. Is community engagement warranted? Is it feasible? What level of engagement is appropriate?
6. What are the social justice implications of this initiative?
7. What are the potential longer term consequences?

APPENDIX B – PRIVACY AND DATA ACCESS GUIDANCE QUESTIONS

1. Who is accountable for the data and where will it be stored?
2. Who will have access to the data?
3. Is there an audit trail to indicate that the data was obtained lawfully?
4. Has sufficient level of anonymisation achieved?
5. Are there any restrictions for secondary processing the data?
6. Can the accuracy of the data be verified?
7. Are the data processing/transformation processes documented and approved?
8. Is there a method where individuals can opt out of being included from the data?