

Refereed papers

An ethical framework for sharing patient data without consent

Robert Navarro BSc Dip KBS
Director, Sapior Ltd, London, UK

ABSTRACT

Background There is no consensus on how to share patient records privately. Data privacy concepts are surveyed and a framework is presented for the safe sharing of sensitive data. It is argued that tailoring the data sharing to the *privacy breach risks* of each project holds out the best compromise for keeping the trust of the public and providing for the best quality data where detailed patient consent is not possible.

Objective To improve the protection of data by reducing privacy breaches and thus enable appropriate patient data sharing without consent.

Framework Any harm arising from data sharing must come from the data being identified, either fully or partially. The first step is an agreement on an acceptable privacy breach risk. Next, proceed to

measure that risk for the proposed data when held by a given recipient. Finally, select from a menu of mitigation strategies (people, process and technical) to achieve acceptable risk. The framework is tested against the current UK approach administered by the Patient Information Advisory Group. **Discussion** The hard problem of non-consented data sharing should be divided into the easier (though non-trivial) ones of *data* and *recipient* breach risk measurement. Directed research in these two areas will help move the data sharing problem into the 'solved' pile.

Keywords: Inference attack, medical records systems, patient data privacy

Introduction

There is no consensus on how to share health data privately. Superficially this is surprising because patient consent cries out as the obvious basis. However, on closer inspection using patient consent as a basis is only ethical when it is prior, informed and understood, freely given and specific.^{1,2} Because occasionally it is not possible to secure one or all of these, an alternative to patient consent is sometimes needed.

In England and Wales access to National Health Service (NHS) data for medical purposes (preventive medicine, medical diagnosis, medical research, provision of care and treatment, the management of health and social care services, informing individuals about: their physical or mental health or condition, the diagnosis of their condition or their care or treatment) without patient consent is controlled by the Patient Information Advisory Group (PIAG; In July 2008 PIAG was merged into a sub-committee of the

National Information Governance Board). Initially set up by the Health and Social Care Act 2001, PIAG control was expected to be a temporary arrangement until patient consent was routinely sought or the information was anonymised or pseudonymised. This is not what has happened. Data access requests must always be approved centrally (with applications being considered only six times per year) regardless of whether the data has been anonymised or pseudonymised.

This paper suggests that the data sharing problem should be viewed through the lens of *privacy breach risk* of the data and its recipient. This simultaneously moves us forward from the status quo and minimises the chance of harm to the patient through that data sharing. It is hoped that *privacy breach risk* qualification and quantification will form the basis of a data sharing consensus and thus play its part in enabling the next generation of evidence-based health benefits.

Background

What is identity and identifiable data?

When some of your very personal information is disclosed where you had not wanted it to be, it is common to feel hurt that a little bit of yourself has been broadcast for all to see and potentially saved for some future time when its use may be hurtful again. It is critical, therefore, when thinking about data sharing to understand the extent to which someone's self or identity is bound up in that data.

Intuitively what other people know about you has passed through one or more of their five senses. In fact that is the only way they can learn anything about you. It follows that a working definition of 'identity' is the collection (or union) of all knowable information about you that can be recorded through the five senses.

It may seem ridiculous that hair colour is part of your identity along with your name. Actually the colour of your coiffure is simply a less selective attribute than name, but it forms part of the wider identity that is recognisable as 'you' by others.

So the extent to which your characteristics can be recorded and replayed determines the extent to which that replay imitates you. Someone with a likeness to you will fool a casual acquaintance. Someone with a likeness to your mannerisms, vocal patterns, approach to problem solving and sense of humour will fool your work colleagues. Alternatively, a remote browser transaction will appear to be from you if it supplies the correct passwords.

In our increasingly electronic world there is often no difference between a database containing captured personal characteristics and the actual person being described. This makes databases of personal or individually characteristic data (especially biometrics) quite

important and the ultimate source of privacy concerns.

What someone knows combined with what's in the data together determine the ability to identify that data

So how does a privacy breach occur? As forensic criminologists say it takes people, opportunity, motive and ability to coincide before a crime occurs. At such a confluence, breaching the privacy of a dataset requires either the attachment of a name to each record (identity disclosure) or the inference of some unique characteristic from the set of records that contain it (attribute disclosure), e.g. learning your neighbour has had an abortion by observing them repeatedly attending a clinic.

If the data carries its own protection via a sensitive field substitution process called pseudonymisation (required of some National Health Service 'secondary use' data by April 2009³), assuming this is implemented robustly, the easiest way to learn the identities in the data is via an inference attack.

Examples are a general practitioner recognising their prescribing pattern within a research dataset or a receptionist spotting their neighbour's unique disability during their work as a receptionist at the local clinic. See Figure 1 for a targeted version of this attack.

Notice that the privacy attack in Figure 1 hinges on discovering someone's unique or characteristic patterns within the data and not on breaking the pseudonymisation protection per se.

What should now be clear is that for data that has had its most identifiable fields replaced (NHS number, name, address, etc.) what someone knows and what is in the data together determine the ability to identify the subjects and therefore breach privacy.

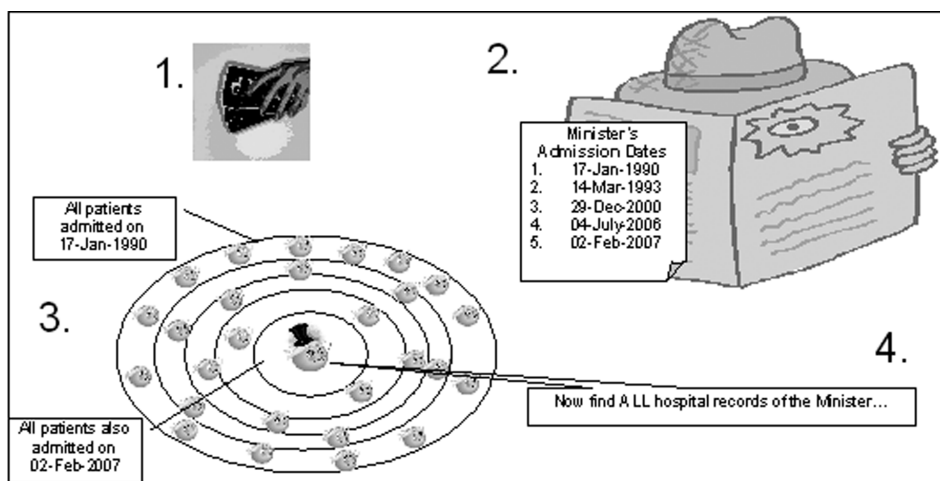


Figure 1 Targeted inference attack on pseudonymous data

Protecting data privacy

So what can be done? Intuitively any process that makes it harder to identify someone's unique characteristics within the data is a good start. In fact this is the approach taken by those valiant enough to attempt both publishing and protecting sensitive data.

Broadly these solutions break down into: query controllers,⁴ (summary) table de-identifiers and (micro) data de-identifiers.⁵ Query controllers remove fields, limit available queries or suppress returned results. Table de-identifiers for national census offices omit outliers, shuffle fields amongst records, smooth or perturb the data or suppress cells with only a few values. Finally data de-identifiers use technologies such as pseudonymisation, encryption, elision, generalisation, perturbation, 'noise' addition, field shuffling or the creation of derived fields. These make it harder to connect unique characteristics to a person by generalising and blurring (losing) some of the data to make it apply to more people.⁶ Privacy loves a crowd.

The more the data is modified the less useful it is

Unfortunately each of the above approaches suffers from the same problem. Each is a general tool trying to preserve the privacy of a dataset for an unknown audience. It would certainly be ideal if a technical solution such as this could be found. However, either too much information is lost in hiding characteristics (preserving privacy) or all individual characteristics are not entirely hidden thus exposing a breach risk.

Rather surprisingly both query control and (summary) table de-identification result in greater data distortion than data level de-identification.⁶ Because releasing protected row-level data also allows for greater analytic freedom, the remainder of this paper will concentrate on the privacy protection of that.

Prior knowledge of a workload allows selective data modification without ruining its utility

Progress can be made if you step back from the goal of a general de-identification solution. By recognising that one project needs pristine diagnosis codes but can cope with blurred demographics (age range instead of date of birth, region instead of postcode, etc.) for example, it is possible to lose less important information and still get useful results.

Different workloads require conflicting modifications

Having agreed to lose some information from the dataset to satisfy privacy requirements for the first project there are now denuded demographics – useless for a detailed study of those demographics. Generally any time information from a dataset is discarded a study somewhere will be prevented.

Not all recipients are equally trustworthy

Is it true to say that a young, inexperienced PhD student in a shared office will husband the patient identifiable information with as much care as a more seasoned researcher with a name and reputation to lose?

If one data recipient is more amenable to being corrupted does that not change the level of risk of giving them sensitive data?

A data-sharing solution must accommodate not only the project's need for pristine data but also the trustworthiness of each recipient and their hosting context.

Every general data protection technology seems to have a weakness

Protecting identifiable data by pseudonymising it leaves the data open to inference attacks (Figure 1). Protecting that pseudonymised data from inference attacks using 'k-anonymity' leaves it open to background attacks.⁷ Protecting that data from some background attacks using 'I-diversity' leaves it open to enhanced background attacks.⁸ Protecting that data from enhanced background attacks using 't-closeness' leaves the data unhelpfully general.

Such a survey of the state of the art in (micro)data de-identification is disillusioning. For those used to the comfort afforded by well-managed encryption this is grounds for doubting the viability of any data-sharing initiative, however promising the upsides are – unless you factor in the breach risk.

Summary: generally there is no one-size-fits-all-users privacy technology for databases

A single database whose contents are accessed by many parties cannot be private for two reasons: it either ignores privacy to ensure its contents are universally useful and/or assumes its recipients are all equally trustworthy.

Corollary: individual solutions are required for each project and each level of trustworthiness

This analysis suggests a solution that can be retrofitted to existing monolithic databases. Individually assess each recipient's needs and breach risks then provide tailored data accordingly.

Framework solution

Basel II inspiration

Risk of a privacy breach is probably the best way to determine how much effort should go into protecting shared data. The situation in banking is analogous: since the Basel Accord of 1988 large banks have wanted to tailor the amount of money they have to set aside in case a loan goes bad. Basel II allowed banks to assess their own risk provided they measured their own operational risk (as well the usual credit and market risks) and showed everyone how they did it.⁹ Risk of failure is the best way to decide how much of a safety net is needed. Similarly, a scientific approach to sharing data privately has three components:

- 1 settle on an acceptable risk level considering the potential harm of a breach
- 2 measure the privacy breach risk of a proposed sharing scheme for each recipient, and
- 3 bridge any shortfall from the risk appetite by selecting from appropriate mitigation strategies – people, process/context and technical.

Acceptable risk level

Is it possible to have water-tight anonymisation with no breach risk whatsoever whilst still sharing data? Unfortunately it is not. The degree of detail necessary for useful research always contains enough unique personal characteristics to allow for inference attacks.

That you do not recognise those characteristics does not prevent someone else from doing so. In other words, the only way to ensure perfect anonymisation is to not share any data at all. Accepting the value of data sharing thus means accepting a degree of breach risk. But how much of a breach risk is acceptable?

Crime is a function of people, opportunity, motive and ability and it should be recognised that breach risk always increases with the number of sharing parties. This means for wider sharing of health records beyond the NHS it will be necessary to either persuade the public to accept a higher privacy breach risk or improve protection beyond what is currently acceptable for sharing within the NHS.

Risk measurement

With an acceptable risk level having been determined you must check to see how far from that goal a data sharing proposal actually is. Given that both the data and the recipient together determine the breach risk, any measurement must quantify both. What is to be measured is the risk of data being identified, either wholly (identity disclosure) or in part (attribute disclosure).

How the data contributes to this overall breach risk has been studied for identity disclosure by Skinner and Elliot and Schlomo,^{10,11} and for identity and attribute disclosure by Duncan and Lambert.¹²

How the organisation contributes to the overall breach risk is likely to be modelled on the way operational risk is measured for Basel II, i.e. causation (people, processes, systems and external factors), measurable events and costs associated with a privacy breach.

Quasi-legal but unethical events such as a UK holder of patient information being served with a US 'Patriot Act' warrant (if they have an American parent company) must also be modelled alongside the more traditional breach risks.

The end result will be a sense of how far away from the acceptable risk level the proposed project actually is.

Appropriate mitigation

This final step is all about picking the most appropriate options from a menu of available risk mitigation approaches to bring the breach risk of the sharing proposal to within acceptable levels.

If your proposed project absolutely needs pristine data then pick people and process options. Conversely, if what is needed is cheap and approximate data then opt for technical de-identification instead. Either way a reassessment of the breach risk will tell you if your option selection (risk mitigation strategy) is sufficient.

It is likely that people and process options will be far more expensive to deploy than technical de-identification. Also sharing fully identifiable data with non-NHS organisations is unlikely to be acceptable (however low their level of risk). Therefore some kind of baseline technical de-identification (probably pseudonymisation) will usually be most cost-effective or may be a required minimum.

Benefits

Low-risk recipients will no longer have to work with less than pristine data. Any organisation, public, private or otherwise has a route to data that is objective and achievable depending only on their ability to demonstrate an acceptably low privacy breach risk.

Discussion

The origin of the reasoning presented in this paper was frustration at a data-sharing process that seems to exclude all but government or academic bodies – regardless of the risk of harm to a patient. This seriously retards innovation. But how could one allow a thousand flowers to bloom and ‘open up’ evidence-based health provision without an increase in privacy breaches?

The answer seemed obvious. Understand thoroughly where the potential harm comes from and create a scalable system incentivised to relentlessly drive down the factors responsible.

The fact that PIAG approval is still required even for anonymous/pseudonymous data is evidence that they acknowledge the data remains identifiable. Without patient consent there is still an ethical need to husband that data on behalf of the patient, i.e. anonymisation/pseudonymisation of the data is not enough.

Adopting a privacy breach risk approach

Were PIAG (or its successor bodies) to institute a privacy breach risk approach to data sharing then these limitations of scalability and unequal access would no longer exist. PIAG or some other NHS honest broker would set and monitor acceptable risk levels, measurement and mitigation standards applicable to NHS, academia, commerce and other bodies. A variety of public and private intermediaries would then ensure implementation and compliance, much as financial auditors do today.

Data recipients would be incentivised to reduce their breach risk because they would have to demonstrate (via audit) an acceptable breach risk environment as a precondition to data access.

The public would be better reassured because attention would be objectively focused on the risk of a breach to their data, with market forces pushing that risk down on a yearly basis.

Comparison with the literature

In the course of researching references for this paper earlier work coming to broadly similar conclusions was uncovered.

The Health Insurance Portability and Accountability Act in the USA (HIPAA) Administrative

Simplification provisions (published in 2006 with references going back to December 2000) uses the risk of a data recipient being able to identify an individual to shape its conclusions.¹³ The main difference between the HIPAA risk concept and those presented in this paper is that HIPAA considers the identification risk inherent in the available data regardless of the recipient. This paper argues that both data and recipient contribute to the ability to identify data and as such both need to be measured.

ISO 17799, a code of practice for information security management, includes the concept of an organisation’s ‘risk appetite’ – the amount of acceptable risk. When confronted with a risk an organisation has four choices; accept the risk, mitigate it, avoid it (stop doing the work) or transfer it to a partner (via insurance). This risk approach is straight forward. Each risk is examined individually and acted upon. The framework presented in this paper is also risk based but is a product of less room for manoeuvre. When sharing health data it is usually not acceptable (or legal) to simply accept the risk of a breach, not sharing is ruled out by definition and legally the responsibility for preventing a breach can not be transferred away from the Data Guardian.¹⁴ This leaves mitigating the breach risk as the only course of action. As has been argued, perfect mitigation is not possible which means the risk needs to be assessed to be proportionately addressed, hence the need for this framework.

In December 2007 the UK Information Commissioner’s Office launched a Privacy Impact Assessment (PIA), a management tool used to identify and examine risks and issues from the perspectives of all stakeholders and then search for a way to avoid or minimise privacy concerns.¹⁵ The PIA seeks to minimise privacy concerns by applying appropriate best practices. In contrast the risk-based data-sharing framework described in this paper guarantees an acceptably low level of privacy risk because that is what is measured. Of course until you can measure the breach risk of a data-sharing scenario the best you can do is apply something like the PIA.

Researchers in health care need to access patient data for epidemiological study and to identify people who might be eligible to take part in research. Much of the medical literature on information security has focused on technical processes; the role of professionalism within health informatics is at best emergent.¹⁶ A conference and workshop set out the issues¹⁷ and subsequently a further conference and workshop have sought to achieve consensus as to how and when individual patient consent should be sought. An interim review of the latter is published within this journal.¹⁸

Conclusion

A scientific approach to sharing private data therefore depends upon being able to measure the combined breach risk of; (1) a dataset and (2) the recipient who will be processing it. This will draw on interdisciplinary knowledge from probability theory, statistical disclosure control and operational risk measurement. Quantitative assessment of privacy breach risks is achievable and is the appropriate framework for sharing patient data when getting their consent is not possible.

REFERENCES

- 1 Lowrance WW. Privacy and health research: a report to the US Secretary of Health and Human Services. May 1997. aspe.os.dhhs.gov/datacncl/phr.htm
- 2 PIAG *Annual Report 2006–7*. www.dh.gov.uk/en/Publicationsandstatistics/Publications/DH_085538
- 3 NHS Connecting for Health. *Information Governance Awareness Workshops*. [www.connectingforhealth.nhs.uk/systemsandservices/sus/SUS-Information.pdf\[AU9\]](http://www.connectingforhealth.nhs.uk/systemsandservices/sus/SUS-Information.pdf[AU9])
- 4 Anderson R. *Security Engineering*. www.cl.cam.ac.uk/~rja14/Papers/SE-08.pdf
- 5 CENEX, Statistics Netherlands. *μ -argus reference manual*. neon.vb.cbs.nl/casc/Software/MuManua14.1.pdf. *τ -argus reference manual*. neon.vb.cbs.nl/casc/Software/TauManualV3.2.pdf
- 6 Sweeney L. k-anonymity: a model for protecting privacy. *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems* 2002;10:557–70. privacy.cs.cmu.edu/people/sweeney/kanonymity.pdf
- 7 Machanavajjhala A *et al.* -diversity: privacy beyond k-anonymity. www.cs.cornell.edu/~mvnak/pubs/ldiversity-icde06.pdf
- 8 Li N *et al.* t-closeness: privacy beyond k-anonymity and I-diversity. www.research.att.com/~suresh/papers/anonymity/anonymity.pdf
- 9 Basel II. International convergence of capital measurement and capital standards: a revised framework. www.bis.org/publ/bcbs107.htm
- 10 Skinner CJ and Elliot MJ. *A Measure of Disclosure Risk for Microdata*. www.ccsr.ac.uk/publications/occasion/occ23.pdf
- 11 Schlomo N. Estimation of disclosure risk for sample microdata using probabilistic modelling. www.statistics.gov.uk/events/gss2005/downloads/PaperF2.doc
- 12 Duncan G and Lambert D. The risk of disclosure for Microdata. *Journal of Business and Economic Statistics* 1989;7:207–17. doi:10.2307/1391438.
- 13 US Department of Health and Human Services Office for Civil Rights. *HIPAA*. www.hhs.gov/ocr/hipaa/finalreg.html and www.hhs.gov/ocr/AdminSimpReg Text.pdf (p.66)
- 14 UK Information Commissioner's Office. Data protection good practice note outsourcing: a guide for small and medium sized businesses.
- 15 UK Information Commissioner's Office. *Privacy Impact Assessment Handbook*. www.ico.gov.uk/upload/documents/library/data_protection/practical_application/pia_final.pdf
- 16 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;76:261–8.
- 17 Frontiers Meeting. *Use of Electronic Patient Records for Research and Health Benefit*. 24–25 May 2007. UK Clinical Research Collaboration and Wellcome Trust, London. www.wellcome.ac.uk/stellent/groups/corporatesite/@policy_communications/documents/web_document/wtd038686.pdf
- 18 Hinds A. Data confidentiality and data handling in research: a workshop report. *Informatics in Primary Care* 2008;16:271–5.

FURTHER READING

H. Nissenbaum. *Privacy as Contextual Integrity*. crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf

CONFLICTS OF INTEREST

Simon de Lusignan is the Principal Investigator and Robert Navarro is a collaborator in a Department of Health sponsored cohort study investigating the effect of Improve Access to Psychological Therapies on the utilisation of healthcare.

ADDRESS FOR CORRESPONDENCE

Robert Navarro
Sapior Ltd
London
UK
Email: phcsg@sapior.com

Accepted October 2008