A CASE AGAINST CENTRALISED SHARED ELECTRONIC HEALTH RECORDS

Andrew Patterson

1) INTRODUCTION

A vision of improved patient care through the sharing of accurate longitudinal clinical data between collaborating health care providers is one of the dreams of electronic health. Improvements to the access and sharing of clinical information can realise benefits of

- Improved coordination of care for patients with chronic conditions; and
- Improved patient outcomes by providing clinicians with accurate and comprehensive patient data at the point of care; and
- Workflow efficiencies through the improved transmission of clinical information; and
- Provide a source of accurate statistical data for quality improvement and medical research.

Health systems at both national and regional levels have attempted to realise this dream through the creation of what is termed a shared electronic health record (SEHR).¹

In both Australia and the UK, a model for a SEHR has developed that involves the construction of a centrally stored database of patient data, fed by extracted summaries of

---

¹ A formal definition of SEHR is “an electronic longitudinal collection of personal health information, usually based on the individual or family, entered or accepted by health care professionals that can be distributed over a number of sites or aggregated at a particular source including a hand-held device. The information is organised primarily to support continuing, efficient and quality health care. The record is under the control of a known party.” - Flinders University, The benefits and difficulties of introducing a national approach to electronic health records in Australia, (April 2000) s 3.1.1.
data entered into local systems.\textsuperscript{2} This model places much of the functionality and power into a central repository, with extremely weak expectations placed on the local systems. In this paper we will take a look at some of the implications of this model and argue the case that many of the problems that are inherent to a centralised SEHR model can be mitigated by designing a strong federated system – highly functional and independent local systems that occasionally reference central infrastructure when needed. The main key to our approach is the establishment of primary care systems that allow external health providers to add and modify clinical data within another provider’s record of a patient. We conclude by discussing the change in mindset that this approach requires and other hurdles for a system such as this.

2) **The Shared Electronic Health Record (SEHR)**

*a) Background*

When viewed purely from a technical standpoint, storing clinical data to allow a longitudinal view of a patient (with strong security mechanisms) is a difficult yet eminently solvable problem. Technical solutions can encompass many different design decisions at many different levels including choices of implementation language, data interface mechanism, data interface format and server architecture.\textsuperscript{3,4,5} This paper is not

\textsuperscript{2} Local systems such as those run by GP’s, allied health providers, hospitals and pharmacies.


an appropriate place to go into the details of these choices, although we will touch upon some of them in section 4.

One technical decision however has a major impact upon the legal, privacy and policy considerations of a SEHR – that of whether centralised\(^6\) computing infrastructure is to be used in the solution and the nature of the data that will be stored on this central infrastructure. Unfortunately, the majority of legal and privacy analysis of SEHR approaches in Australia and the UK have analysed a model where the decision to have \textit{clinical} data in a centralised repository has already been made.\(^7,8,9,10\)

In this paper we would like to look at the legal and privacy issues raised by the centralised SEHR model. We will find that many of the issues are caused by the need for transfer of data from health care providers to a third party organisation running the centralised system. If a technical solution could be designed that obviated the need for a centralised store of clinical data, many of the privacy and legal issues disappear. We will argue that such a solution is more than possible, and has other benefits relating to improved monetary compensation for the providers responsible for patient records, and increased competition for medical IT services.

\(^6\) Centralised does not necessarily mean one single server – Google provides a centralised search engine service yet has many thousands of machines distributed around the globe providing the service.

\(^7\) This is in no way the fault of the legal or privacy analysts themselves – their scope for discussion is obviously limited by the system constraints they are presented with.


b) A brief history of HealthConnect

HealthConnect is a major SEHR project in Australia.\textsuperscript{11} Its origin lay in the establishment of a National Electronic Health Records Taskforce by the State and Federal health ministers in 2000.\textsuperscript{12} The report made several recommendations regarding the importance of establishing nationwide standards, infrastructure and uniform legislation regarding data protection. This infrastructure work is ongoing under the auspices of the organisation NEHTA.\textsuperscript{13}

The key recommendation was that the health ministers should agree “to the establishment of a health information network for Australia”.\textsuperscript{14} The proposed architecture consists of each encounter with a health provider generating a detailed encounter record. This is the type of record that is already recorded by clinical information systems at the point of care. Each encounter would also generate a summary record that would be sent to a centralised server, subject to patient consent and other security mechanisms. The collection of summary records would be viewable by other health providers in the system, with different views of the data based on the type of health service provided. De-identified data from the summary records could also be used for public health analysis.

\-----------------------

\textsuperscript{11} It is not clear that HealthConnect as a program is an ongoing concern because its funding has not been renewed. Rather, the money has been committed to the organization NEHTA which is carrying on similar work. See NEHTA, \textit{Shared Electronic Health Record Fact Sheet} <http://www.nehta.gov.au/index.php?option=com_docman&task=doc_details&gid=103&Itemid=139&catid=2> at 14\textsuperscript{th} June 2007.

\textsuperscript{12} National Electronic Health Records Taskforce, \textit{A Health Information Network for Australia}, (July 2000).

\textsuperscript{13} The NEHTA work program involves building blocks such as provider directories, patient identifiers and terminology sets.

\textsuperscript{14} \textit{A Health Information Network for Australia}, above n 12, XXIX.
The resulting work program from these recommendations was called HealthConnect. The important feature of the HealthConnect architecture is that it requires some form of centralised and third party infrastructure for storing the clinical summary records that are produced at each encounter. The exact content of the centralised records has not been standardised but the primary areas of interest are surrounding current patient conditions, allergies and medications. The physical architecture has not been formally decided either but is tending towards multiple clinical stores (perhaps on a regional basis), run by either one central organisation, or with each store run by separate regional organisations.\(^{15}\)

### 3) Legal Issues of Shared Electronic Health Records

A comprehensive report on the legal aspects of HealthConnect was released by Clayton Utz in 2005.\(^{16}\) As it is the most comprehensive discussion of the legality of shared health records in an Australian context, we will follow its basic structure to highlight the differences between centralised and federated models for SEHR. We will use the HealthConnect architecture to represent an example of the centralised model. Without yet detailing an exact model, we consider a federated model to be one in which clinical data is only ever stored by organisations responsible for the provision of healthcare. This may require some central infrastructure support (such as an index to let health providers find other local health providers), but has a key difference from HealthConnect in that no clinical data is stored outside of systems under the control of health providers.

---

\(^{15}\) HealthConnect, *HealthConnect Systems Architecture 0.9*, (July 2003).

The report identified eight broad areas in which there are legal issues:

a) Legal validity; and
b) Governance; and
c) Intellectual property; and
d) IT and e-commerce; and
e) Liability and indemnity; and
f) Custodianship and control; and
g) Privacy and consent; and
h) Procurement (not discussed in this paper).

Some of these areas are orthogonal to the design of the system in that the legal questions raised or analysed do not depend on the model of SEHR. We will briefly review some of these areas, and then look more closely into those legal issues that are affected by the design of the system.

**a) Legal validity**

There are generic legal questions regarding the basis of electronic health records as legal documents. Each jurisdiction has enacted legislation that allows suitable electronic mechanisms to take the place of paper based records, written communications and signatures\(^\text{17}\) and hence a well designed electronic health record can meet the legal requirements imposed on health providers. Prescriptions form a special type of written document and legislative changes will be necessary to enable electronic signatures on

\(^{17}\) *Electronic Transactions Act 1999* (Cth).
electronic prescriptions to meet the requirements for authorisation and dispensing of medications.

The choice of SEHR model should have no effect on the legal validity of the records contained within.

**b) Governance**

Any computer system must have an organisation in charge of its day to day running. Possibilities for this organisation are to assign it as a function to a government department, the creation of a statutory authority, or incorporation as a separate company. No matter what SEHR model is undertaken, there is a requirement for some level of centralised infrastructure such as certification authorities (to validate and authenticate electronic signatures) and health provider directories (to allow the electronic addresses of suitable health providers to be located). It is not possible to recommend a particular form of governance based purely on the SEHR model except to note that the larger the functionality of a centralised system, the more important the decision of governance becomes.

**c) Intellectual property**

There are two broad areas of intellectual property concern – ownership of the intellectual property of the software and ownership of the intellectual property of the data stored in the system. In terms of the rights for the software, copyright in software is generally vested in the creator of the software unless transferred explicitly through contract. There is a clear case for software vendors to retain copyright in their software to enable them to leverage their work for other software projects. However, there is also a competing
interest from the purchasers of software to be able to modify and improve the software they have purchased without being held to ransom by the original vendor. In the industry generally, copyright is not transferred to the purchaser, but some form of broad license agreement is reached permitting changes to the system (or even access to the source code of the system) by the purchaser. As with the issue of governance, the exact resolution of these intellectual property issues is much broader than the issue of the SEHR model chosen - though we would once again note that the larger the functionality of the centralised system that is being purchased, the more crucial these decisions become.

The issue of intellectual property in the records themselves will be dealt with in section f).

**d) IT and e-commerce**

The legal issues in this area surround data quality, data security and data availability. Organisations that hold data are subject to various privacy principles – we will assume that any organisation dealing with shared electronic health records will either be subject to a local health specific privacy statute,¹⁸ or failing that a generic set of privacy principles.¹⁹

One common privacy principle requires holders of data to take reasonable steps to protect personal information from unauthorised access.²⁰ A centralised system has an advantage in this respect because any organisation running such a key clinical system would have


¹⁹ *Privacy Act 1988* (Cth).

²⁰ Ibid, NPP 4.
the resources to ensure adequate layers of security for the system. On the other hand, a centralised system has the downside that in event of a breach there is potential for a massive number of people to be affected. In comparison, a federated approach requires each site (with presumably less access to staff expertise and resources) to ensure adequate security for its computer systems, yet a breach of the system will not affect nearly as many people. Given the number of organisations in other industries that can successfully protect their computer systems, it is probable that adequate data security can be obtained by organisations in a federated approach to medical records.

Data availability is the legal issue of whether downtime of the system (and hence an inability of a health provider to obtain information for care) could potentially lead to legal liabilities for those organisations running the computer systems. This is an issue that may develop in the future but should surely not be of a concern in the initial development of shared records. Given that the alternative to an electronic shared record is no shared information at all, health providers will have to handle system downtime exactly as they handle situations currently - by asking patients and their family members for detailed clinical histories. A centralised system has an advantage here in that there are potentially less ‘moving parts’ where system faults can develop.

Data quality is a key issue that is poorly handled in a centralised shared health record. Privacy principles require that reasonable steps are taken to make sure information is accurate, complete and up to date. The very nature of the centralised architecture is that all contributors are responsible for their contribution to the record, yet no-one is actually responsible for the data quality of the aggregated records. This is akin to having everyone

21 Privacy Act 1988 (Cth), NPP 3.
throw pieces of paper into a filing cabinet presuming it will organise itself. Another issue of data quality is that all information in a centralised shared record is secondary information. This means that for instance if a specialist were to delete an allergy from the list of allergies stored in a shared record, this change would not automatically flow back to the primary copy of the data stored on another GP’s system who contributed that allergy to the record. This is not to say that secondary copies of information are worthless – just that where possible operations should be done on the primary copy of information. In a centralised system this is not possible as all data is secondary.

A federated approach to data quality says that each provider is responsible for the data quality of the information contained within their system. Each provider may contribute secondary data to other providers to help them make clinical decisions, but the organisation of that data is then the responsibility of the provider who owns the system. This does not mean that a provider takes on ‘authorship’ of the data contributed to their system – the secondary data contributed by another health provider should be legally attestable to the contributing party. However, the provider who holds the copy should act to make sure the organisation of such data is sensible, and act to ensure the overall record is accurate, complete and up to date.

The issue of working on primary copies of information is as difficult in federated systems as it is in a centralised system. Whilst each health provider may have a list of what they believe to be allergies of the patient, clearly the reality is there is only one patient – and therefore logically only one list of what the patient is actually allergic to. One possibility for approaching this aspect of data quality in a federated system is that one health
provider might be designated as the provider who holds the primary copy of information of this sort. We revisit this idea in section 4a.

**e) Liability and indemnity**

A shared health record provides the possibility that health providers may be held negligent for actions they perform based on incomplete or incorrect information in a shared record. There is then a legal question as to how the liability will be apportioned between the users of the SEHR (the contributing health provider and the health provider who used the data). In a centralised system, health providers are responsible for each individual contribution they make – yet no-one is responsible for the overall picture provided by the collected records. It is inherent to the nature of health records that some information becomes irrelevant merely through the passage of time – at the time of diagnosis a health provider could make a completely accurate contribution to a shared record stating that a patient is suffering from chest pains. The same health provider may not feel obliged to make a summary statement three weeks later stating that the patient is no longer suffering chest pains. Yet no-one is responsible for checking the ongoing accuracy of the summary statements contained in the shared record. Chest pain may be listed as an ongoing condition of the patient for years into the future, perhaps adversely affecting the accuracy of other diagnoses made by health providers.

---

It is this lack of responsibility for the *collected* information that muddies the waters when assessing the liability for health providers who have contributed and used information in the SEHR.

In contrast, in a federated approach, a health provider would still be responsible for the accuracy of the summary records they produce – but the health provider in whose system the information is placed would be responsible for the information as a collection. In line with the example above, this would mean that the health provider should ask at the next encounter about the patient’s chest pain and if necessary make the record accurately reflect the real situation.

There may be some mechanism needed to distinguish between information that has been placed into the record but which has not yet be ‘sighted’ by the holding health provider. The balance here is between having an accurate authoritative record, and the burden of requiring health providers to actively monitor patient records outside of normal encounters – current funding regimes only recognise work done in the context of an actual health encounter.

**f) Custodianship and control**

Doctors in Australia have fiercely guarded their ownership and control over patient records. The landmark decision of *Breen v Williams*\(^{23}\) established that patients have no proprietary rights in their own medical records. Recent statutes have given patients some rights of access to their records,\(^{24}\) though ownership is still presumably vested in the

\[\text{23} \quad \text{*Breen v Williams* (1996) 186 CLR 71.}\]

\[\text{24} \quad \text{Health Records Act 2001 (Vic).}\]
health provider who has created the record. A centralised system introduces new legal issues because summary records are held by a third party who operates the shared health record infrastructure. There are questions as to whether the collation of summary records in a database by the SEHR conveys some copyright to the infrastructure owner, over and above copyright in the actual data.\(^{25}\) There are also legal questions as to which organisation would be responsible for satisfying freedom of information requests for information in the shared record.\(^{26}\)

A federated approach is the superior in this regards because there are no third party organisations holding any clinical records. The normal legal principles that apply to health providers and their records still apply. The only new legal issue that arises is in regards to the copyright of a summary that has been contributed to another providers’ system. It should be possible to construct a legal framework that adequately addresses this issue.

\textit{g) Privacy and consent}

\textit{i) Privacy}

The most crucial failing of centralised SEHR models is their inability to assuage the suspicion of consumers and health providers regarding third party organisations holding clinical data.\(^{27,28}\) Patients seem comfortable with the existing privacy arrangements they

\(^{25}\) \textit{HealthConnect Legal Issues Report}, above n 8, 32.

\(^{26}\) Ibid, 36.

make with health providers – they freely share clinical information with the provider who is then bound by a confidentiality duty to keep that clinical information private. This does not preclude the sharing of clinical information with other health professionals to provide care for the patient – no patient would be surprised that nurses at a hospital, or other staff in a GP clinic would have access to their record. Further, they would expect providers whom they encounter to share information from organisation to organisation if they are all involved in the patient’s care (information travelling from a GP to a specialist for instance). So it is not the fact that information is being shared or exchanged that worries patients. We believe the problem lies in an understandable unwillingness of consumers to extend trust to a third party organisation with whom they have no direct relationship. It is not clear that this lack of trust could be overcome by ploughing ahead with a centralised SEHR model. It is possible that trust could be built through operation of a real live system over a sustained period of time, assuming the system suffers no privacy breaches. A federated model is neutral with respect to privacy in that all existing confidentiality and privacy arrangements between health providers and patients remain unchanged.

ii) Consent

A recurrent question in all SEHR systems is whether consumers should be required to consent to be in the system, or whether they should all be automatically put into the system and then have to follow a procedure to have their records removed if desired.

---

The legal position in Australia tends towards requiring an opt-in process. However, various SEHR projects have gone ahead with an opt-out approach – indeed one of the HealthConnect trial projects in NSW required a last minute amendment to the *Health Records and Information Privacy Act* to be passed guaranteeing health providers legal immunity for participating in the opt-out HealthConnect trial.

The choice between opt-in or opt-out is not dependant on the SEHR model used, but we suspect it is more likely that providers and patients involved in a federated model would collectively chose an opt-in approach.

**iii) Secondary usage**

One potential benefit of centralised SEHR data is that it could be used in a de-identified form for public health studies without explicit consent of those patients whose data is involved. It has been shown that requiring explicit consent for even de-identified data skews the results of public health studies. Therefore there is clearly a need for government organisations to have access to statistical data regarding health trends in various communities and for researchers to have access to de-identified data without explicitly requiring consent from each individual patient. However, there is no evidence that collecting this data can only be achieved with a centralised system. It may be wishful

---

29 *Health Records and Information Privacy Act 2002* (NSW), HPP 15.

30 *Health Records and Information Privacy Regulation 2006* (NSW), regulation 3.

31 Steven Woolf, et al., ‘Selection bias from requiring patients to give consent to examine data for health services research’ (2000) 9 *Archives of Family Medicine* 1111.

for a government department to imagine performing this statistical research on a
centralised system staffed by willing health administrators rather than asking
cantankerous GP’s for their data.

A federated approach is similar to the current situation where government goes to each
health provider and asks them for de-identified datasets of their patients. Already some
data is beginning to flow out of GP practices\(^{33}\) though there are questions about the
quality of GP data.\(^{34}\) All in all – the desires for governments and researchers to have a
centralised store does not convincingly mandate that approach because there are other
ways of collecting public health data - there seems to be no reason to place the ease of
access of researchers above the concerns of patients or health providers.

4) **A NEW MODEL**

We have examined various legal issues surrounding SEHR models and found strengths
and weakness with both centralised and federated models. In areas of major importance
such as privacy, custodianship and data quality, we would argue that federated models
are clearly superior. In no area does it appear that centralised models provide a markedly
better solution to federated records. Federated models have a higher complexity of
implementation and require more use of IT standards but it would be very short sighted to
make a long term commitment to a large centralised system just because of upfront costs.

\(^{33}\) *Australian Family Physician* 4.

\(^{34}\) Judith Jones, et al., ‘Missing and Incomplete Data Reduces the Value of General Practice Electronic
Medical Records as Data Sources in Research’ (2007) 13 *Australian Journal of Primary Health* 74.
Incidentally, these concerns over quality level would equally affect centralised shared health records.
At the minimum, various federated approaches should be discussed and analysed by IT, privacy and health policy experts in the same way that the centralised model of HealthConnect has been analysed over the past five years.

**a) The collaborative electronic health record (CEHR)**

We would briefly like to propose a possible model for a workable federated electronic health record. Unlike other models, this model acknowledges the inherent asymmetrical nature of a realistic shared record. Rather than view every health provider as an equal provider of health care data - all contributing to some uncontrolled centralised store, the CEHR model would designate one particular health provider as the centre point for the coordination and storage of longitudinal data for the patient. In an Australian setting, the obvious candidate would be a patient’s GP, who already acts as a focal point for most of their health care related activities. Consider then a system whereby a patient could associate their Medicare number with a particular GP who was willing to accept data into the providers’ computer system regarding that patient. This provider would be the location of the patient’s collaborative electronic health record.

It should be noted immediately that nothing in our model requires patients to attend only one GP. A patient has the choice to have encounters with any health provider they wish – at the end of the encounter, the patient can ask that a summary of the encounter is dispatched to their CEHR. The patient’s Medicare number will help the provider’s computer system locate the CEHR service in which data is to be stored or accessed. For the health provider, the CEHR service could give access to any patient data that the patient and CEHR providing GP had enabled for viewing. It would be possible that some health professionals would have a ‘write only’ view of the CEHR – a physiotherapist
might be able to contribute a report back to the CEHR but not be able to see any diagnoses or medications. The patient and CEHR GP would be in charge of decisions like these at all times.

If the information is of a sensitive nature, the patient could choose to not have that information shared back to the CEHR service at all. In the best case, where patients and
providers embrace the concept, the patient builds up a reliable, accurate lifelong health record. In the worst case, where patients remain secretive about their data, the patient is no worse off than in the current Australian health care system where all data is stored in separate silos.

In fact, the model recognises that if patients are to have the freedom to choose any provider and to retain control over their medical information, they must at some level deal with the consequences of those choices. So, if they wish to maintain some sort of comprehensive life long electronic health record, at some point they need to choose a particular GP to provide that service. Similarly, they will need to encourage their health providers to commit summary information back into their CEHR. If they don’t see the value in such a service then there is no requirement for them to take part in it. It is our opinion however that those who will stand to benefit the most from coordinated care, such as those with chronic diseases, are those most likely to feel comfortable choosing a particular GP to store their CEHR. Presumably, the benefits of the system will become obvious to others over time – if no benefits become apparent then perhaps shared electronic health records are a concept that are fundamentally undesirable.

From an IT perspective, a federated model such as CEHR would require a commitment to interoperable standards by vendors of health care software. There would be an important role for the government in choosing these standards and also in ensuring an accreditation system to make sure differing vendor’s systems were compatible with each other. A federated approach however gives vendors a great scope for competing with each other in all areas that do not require standardisation. Therefore, whilst the data that is exchanged between systems would need to be standardised, the interfaces available to consumers
and health providers around the system could be a good source of competition. Similarly, the CEHR concept provides a competitive driver for GP practices with regards their computerisation. A GP who provides an impressive interactive web interface to records for their patients, and who invests time and money in establishing a solid CEHR service may find more consumers willing to visit them as a GP. Those GP’s and health providers who are unwilling to participate in the system may find themselves at a competitive disadvantage.

Finally, the CEHR model provides an opportunity for the government funding system to adequately compensate GP’s who provide record keeping services for a patient. It would be possible to count the number of patients who designate a particular GP as their CEHR service – this could lead to some level of funding going to this GP for providing the service. The funding could encourage GP’s to perform a regular review of the data quality and accuracy of their patient’s records (outside of that performed in normal encounters).

**b) Problems with the CEHR**

A change in model brings with it a new set of problems – technical, political and legal. We briefly discuss some of these problems and possible solutions.

**i) Opening up GP systems**

The CEHR model requires GP’s to go to an IT architecture that allows read/write access to patient data from outside their internal network, though obviously subject to suitable access controls and security. Most current GP computer networks are not constructed this way because it would be a needless security risk to expose a system to the Internet for no
benefit. It would be up to the IT industry and vendors to convince GP’s that it possible to have computer systems exposed to the Internet with adequate levels of data security.

**ii) Allowing others to place data in a GP’s records**

The CEHR model requires GP’s to allow other providers to enter data directly into a patient record in the GP’s system. Obviously, we are not suggesting that just anyone would be able to enter data into a patient record. Access would be strictly controlled through mechanisms under the control of both the patient and GP. All data in the patient record would be legally attestable to the provider who had entered it. However, it is a fundamental shift in mindset for GP’s to consider that an external person be given the facility to enter data into their records. It is not clear how this change in mindset would be achievable.

**iii) System availability**

The CEHR model assumes that GP systems are “always on” and available for reading and writing. Whilst broadband penetration in Australia is quite good, care must be taken to retain equity of access to medical services for communities that may not have quality broadband infrastructure.

**iv) Record transport**

A true lifelong longitudinal record must encompass the fact that at various points in a patient’s life they are likely to move between geographical regions. A significant change in location could make any form of physical contact with the GP in charge of the patient’s CEHR impracticable – it would therefore make sense to make a more local GP
in charge of the patient’s CEHR. It would be useful to have some electronic method of transferring a CEHR from one GP to another.

5) Conclusion

There is a strong belief that longitudinal electronic health records can be a driver for improved clinical workflows and an improved standard of care for patients. However, many large government projects in this area have concentrated on a single model for shared electronic health records, that of a centralised computer system fed by data from other clinical systems. As we have seen in this paper, there are many concerns regarding this centralised model in the areas of privacy, custodianship of data and data quality.

In comparison, a federated approach removes the need for the storage of clinical data in a centralised repository, and is a very legally neutral way of handling the sharing of information – existing laws and practices cover the vast majority of legal issues in the federated model.

We have proposed a federated model which we have dubbed the collaborative electronic health record. The key point of the model is in recognising the inherent asymmetry required in a storage system if one wants to achieve the aims of coordination and continuity of care. By designating a GP system as the preferred location for the storage of medical records, a longitudinal record can be built under the full control of the patient and their designated health provider.
6) **BIBLIOGRAPHY**

**a) Articles/Books/Reports**


Flinders University, *The benefits and difficulties of introducing a national approach to electronic health records in Australia*, (April 2000).


Woolf, Steven, et al., ‘Selection bias from requiring patients to give consent to examine data for health services research’ (2000) 9 *Archives of Family Medicine* 1111.


b) Case Law


c) Legislation

*Electronic Transactions Act 1999* (Cth).


*Health Records and Information Privacy Act 2002* (NSW).

*Health Records and Information Privacy Regulation 2006* (NSW).

*Privacy Act 1988* (Cth).

d) Other sources


NEHTA, *Shared Electronic Health Record Fact Sheet*  
