IT-BASED COLLABORATIVE HEALTHCARE INITIATIVES: A LEGAL ANALYSIS

Moira Paterson
Kay Jones
Monash University

Technology offers the potential for collaborative treatment of chronic diseases involving clinical partnerships between multiple health care providers based on web-based care plans. However, collaborative regimes may increase the potential for medical negligence suits. Possible issues include responsibility for ensuring the appropriateness of any care plan, the accuracy, security and continued integrity of any information entered in the system and responsibilities to follow up patients.

INTRODUCTION

This article explores legal issues arising from the use of collaborative health care plans supported by information technology, especially electronic health records. The convergence of collaborative care models and electronic health records was highlighted in nine new eHealth projects based on the new personally controlled e-health records (PCEHRs), announced in March by the Minister for Health and Aging (Roxon 2011). These projects include the roll out of PCEHRs to patients with chronic illnesses, to help facilitate team-based care.

This article draws on a research conducted over the period 2007-9 for a major project which piloted the use of a broadband system operated by a private sector intermediary to facilitate the development and electronic transmission of electronic care plans to care teams treating patients with chronic diabetes in regional Victoria and Western Australia (see DBCDE 2011). The issues have been further explored from a multi-disciplinary perspective in a roundtable discussion of clinical, legal and ethical experts. The full results of the roundtable were published in June 2011 (Paterson et al 2011).

BACKGROUND

The large and growing cost of chronic disease is encouraging the use of collaborative healthcare models. Chronic disease is expected to grow significantly in line with the aging of the population and increasing prevalence of shared risk factors such as overweight and obesity, poor nutrition and physical inactivity. On current projections Australian health care expenditure for cancer, cardiovascular disease and diabetes will nearly triple from $14.4 billion in 2002/03 to $41.3 billion in 2032/33 (Goss 2008).

Local and overseas research suggests that collaborative, multidisciplinary care may help in the treatment of patients with chronic illness (see for example Zwar 2008, Rothe 2008). Successive Australian governments seem to agree. In 1999, general practitioner (GP) enhanced primary care (EPC) item numbers were introduced for enhanced multidisciplinary primary care planning, requiring collaboration between GPs, other providers and patients with

chronic illnesses. In 2005 new item numbers for general practitioner management plans (GPMPs) and team care arrangements (TCAs) were added. GPMPs are used for patients with a chronic illness who would benefit from 'structured care',which is based on a structured preventative approach as opposed to episodic acute management. TCAs are intended for patients needing complex care involving collaboration among providers. They allow patients to claim rebates for allied health (healthcare provided by clinical health professions other than medicine, dentistry and nursing) and dental care. According to Medicare statistics, GPs prepared more than 645,000 GPMPs in 2005–06 and almost 300,000 multidisciplinary care plans (enhanced primary care and team care arrangements) (Medicare Australia).

At the same time, the Australian government developed eHealth strategies. In 2005, the National E-Health Transition Authority (NEHTA) was created to coordinate the implementation of these strategies. NEHTA's Strategic Plan for 2009-2012 identifies four priorities: "... to develop the essential foundations required to enable e-health; coordinate the progression of the priority e-health solutions and processes; accelerate the adoption of e-health, and lead the progression of e-health in Australia" (Dearne 2009).

NEHTA has developed unique health identifiers for all patients, practitioners and Australian healthcare organisations and established the Health Identifiers Service within Medicare on 1 July 2010 (NEHTA 2010). Health identifiers are numbers assigned to uniquely identify healthcare providers and recipients. The *Healthcare Identifiers Act 2010* permits the use of identifiers only for healthcare and related management purposes, and penalises their misuse.

Healthcare identifiers provide an important building block for the PCEHR announced in the May 2010 Federal Budget. It is intended that all Australians will have the option of applying for a PCEHR by July 2012 (Woodhead 2011). PCEHRs will contain summaries of patients' health information such as regular medications, key elements of treatment history and current diagnoses and provide a means for secure access to patients' eHealth records. The Government intends to provide "rigorous governance and oversight to maintain privacy" although the precise measures for this have not been clearly spelt out.

One of the new PCEHR implementation projects involves patients who are chronically ill. The Medibank Private Limited Project...

> will implement a consumer-oriented portal, which integrates consumer entered information into a 'Health Book'. The 'Health Book' will be initially made available to all Medibank Private customers and their healthcare providers enrolled in Medibank's Health Management and Chronic Disease Management programs (Commonwealth Department of Health and Aging 2011).

The use of electronic health records for the collaborative treatment of the chronic disease diabetes was illustrated via the trial of the CDM-Net (Chronic Disease Management Network) project.[1] CDM-Net uses shared electronic care plans as a basis for the multidisciplinary treatment of diabetes patients. A secure, collaborative web-based service is used by several practitioners to create, share, track, monitor, and manage patients' care.

Key elements of that system include:

- an Intelligent Application Service, which provides support for the GP, care team, and patient; by providing an interface to enter and read information;
- a Health Services Bus, which provides an open infrastructure to enable different broadband-based services and other systems to 'plug in' to the network and to communicate and interact with each other; and
- connectivity infrastructure, which allows applications and existing systems (such as GP's clinical desktops and hospital systems) to securely connect to, and exchange data, with the Bus (*CDM-Net Final Report)*.

A vital feature is the collection and sharing of information about each patient, including medications and immunisations, and inactive as well as currently active health problems. This information comes from a variety of sources, including the GP's clinical desktop, other

members of the care team, the patient, some hospitals and emergency services, and some pathology laboratories.

The system uses standardised templates to create draft GPMPs and TCAs, and GPMP and TCA reviews, for approval by the GP. It also continuously monitors patients' health parameters, such as blood glucose levels and medications, and is designed to assist them adhere to their care plans by sending SMS reminders and alerts.

Although collaborative health care plans, supported by electronic health records, offer significant benefits, they also raise legal issues in two main areas: privacy and security, and negligence.

PRIVACY AND SECURITY

Information privacy laws limit the collection, use and disclosure of personal information. They give individuals the right to access their own information and to require incorrect or misleading information to be amended. The aim is to allow individuals to exercise informed control over the collection and processing of their data. For example the Victorian *Health Records Act* 2001 contains a set of Health Privacy Principles which, among other things, limit the collection, use and disclosure of identifiable health information.

The right to privacy is recognised as human right and is generally acknowledged as being an important aspect of autonomy and human dignity. Australia is a signatory to the International Covenant for Civil and Political Rights which requires in Article 17 that everyone has a right to the protection of the law against "arbitrary or unlawful interference with his privacy". The Victorian Law Reform Commission (VLRC) has said:

> Privacy is invariably associated with the terms 'autonomy' and 'dignity'. .. autonomy can be defined as self-government and dignity as that human quality which distinguishes people from property; that which makes people 'subjects' not 'objects' (VLRC 2002).

Information privacy also serves an important instrumental value in protecting individuals from discrimination, for example by employers. This issue generally receives most attention in the context of genetic information (Mainsbridge 2001).

Health information is a particularly sensitive form of personal data. Some conditions or treatments carry special stigma. For example:

> Mental health consumers are particularly sensitive to data security, confidentiality and privacy issues. This is because of the prevailing stigma and discrimination which surrounds matters which may arise in the mental health field, like clinical diagnoses, drug and other addictions, sexual practices, dysfunctional relationships and antisocial behaviours (Rivers 2010).

Likewise, women believe information about pregnancy termination is sensitive because it may result in stigma based on preconceptions about their sexual behaviour. Even information about less inherently stigmatising conditions or treatments can result in discrimination, for example, by an employer who prefers to employ individuals with no past history of major illnesses or injuries.

If privacy issues are not appropriately addressed, lack of patient candour can undermine healthcare. As noted recently by a clinical leader at NEHTA,

> Every doctor is concerned about the clinical risks if patients are reluctant to share information with them because they thought – somewhere, sometime – that information might be accessed inappropriately (Lord 2010 and see Terry 2007).

The rationale for the use of electronic health records is that they facilitate sharing of detailed information about patients. It is not surprising therefore that they generate privacy concerns, given the sensitivity of the information that they contain. What is of fundamental concern over and above any issues relating to security, however, is that they enable the sharing of

more information than might normally take place in the context of a team care arrangement based simply on referrals.

A Newspoll phone survey conducted in March 2010 found that while patients are generally in favour of an individual electronic health record, they also want to be able to exercise control over what is in it and who gets access to it. Of the 1208 randomly selected Australians aged 18 years and over for this study commissioned by CSC (an IT service provider), 89% nominated the ability to select which healthcare providers view their information as being of value (Pettigrew 2010). For example, they may prefer that ancillary care providers do not have automatic access to more sensitive information such as information about past mental health issues (see Paterson and Mulligan 2003; Sankar, Mora, Merz and Jones 2003). There are a number of different mechanisms that may be used to regulate information sharing but to date these have been considered primarily in the context of electronic health records more generally (see Coiera and Clarke 2004; Paterson 2004).

The collection and use of identifiable health information is regulated in Australia by a tapestry of information privacy laws.[2] GPs and other private sector health providers are currently regulated via the private sector national privacy principles in the Privacy Act 1988 (Cth). (In 2010, the government issued an exposure draft for a combined set of Australian Privacy Principles which would replace both the private sector National Privacy Principles and the Information Privacy Principles which regulate Commonwealth public sector bodies.) In the ACT, New South Wales and Victoria, health providers are also regulated via sui generis health records laws. [3] State and territory public sector health providers are regulated by state and territory laws in most states and territories.

While these laws differ in their detail, they embody principles which, among other things, impose limits on the collection, use and disclosure of identifiable personal information. In the case of the private sector and sui generis health records laws, data may generally be collected only with consent. In addition, data collected may only be used consistently with the purpose of collection, except with consent or subject to other limited exceptions. Other requirements include the need to ensure that data is relevant and up-to-date and that it is kept secure.

It follows that data should be collected only with informed consent and used and disclosed consistently with the purposes for which it is collected. Informed consent requires that patients should have an accurate understanding of what information is being processed for sharing on each occasion that the information is transferred into the system. They also need to have a general understanding of how shared records are used and who has access to them. The time required to do this must be factored into the time available for consultations. Another significant matter that is often overlooked is the extent to which data on the shared record can leach into the health provider's own treatment records.

What is collected should be relevant to the purpose of collection, that is, the patient's treatment within the context of the care plan. It should not exceed what is required for effective patient treatment. The extent to which this can be achieved may be affected by constraints inherent in the software used on GPs' computers. To the extent that the software has not been developed with selective sharing in mind, as is currently the case, what may be required is a wholesale transfer of existing information with selective omission of specific data taking place prior to the transfer of information. While it might be expected that a GP would be alert to the sensitivity of information in categories such as sexually-transmitted diseases, the sensitivity of specific information may vary according to the patient and the context.

The use of computer systems linked to the internet or accessible by people other than health care providers raises further security issues (Win Khin Than 2005). These may affect other professionals, laboratories or owners of software used to record data. Transmission of data to third parties via email or in other electronic forms raises issues about the security of transmission and the need for encryption. Privacy laws do not provide details of what is required because needs vary according to context. In general terms, it is important to ensure there are security measures in place appropriate to the sensitivity of medical records. These may include authentication mechanisms that comply with current standards for health records

(see OFPC 2001), and measures addressing the issue of third party access by any information technology provider, for example via contractual provisions and the implementation of appropriate protocols.

NEGLIGENCE

Negligence issues may also arise due to the use of a shared treatment plan and reliance on an IT-based system of communication and patient management (Terry 2004; Evans et al 2008). It is therefore important to consider carefully what duties are owed to patients and the nature of the duty of care that arises in each case.
The key issues fall into five broad groups:

- computer error;
- the suitability of a system of treatment based on a computer-generated care plan;
- miscommunication;
- shared responsibility; and
- duties to recall and follow up patients.

Computer error

Electronic care plans are dependent on effective software design, the use of computer hardware appropriate to the effective functioning of the system, the correct input of data and the maintenance of appropriate security measures to prevent authorised access to patient data and to guard against viruses and other malware which can delete or alter patient data. Failures in any of these may result in liability where they jeopardise patient treatment.

Suitability of care plans and reliance on them

A care plan sets out a proposed schedule of treatment. This may provide a document that can be used by the patient in litigation.

A decision of the Victorian Court of Appeal makes it clear that treatment plans must not only accord with what a respectable body of other professional opinion says was appropriate to offer but must also be appropriate in light of the particular circumstances of the patient.[4]

In the case of a care plan generated using a standardised template, therefore, it is important to ensure both that the template is based on current best practice and that it allows sufficient flexibility to address the specific needs of individual patients.

A further issue is the extent that the care plan can, or should, be relied upon as a sole basis for treatment. This may depend on which team member is using it. If a team member is involved in a patient's treatment only as part of the care team, such as a podiatrist involved in the treatment of a patient only in respect of the symptoms of diabetes, then reliance on the plan may be appropriate. The position would be quite different, however, for a GP involved in other aspects of a patient's treatment as well.

The case of *O'Shea v Sullivan and Macquarie Pathology* illustrates the dangers of incorrect reliance on a single source of information, although it was not concerned with a care plan.[5] The doctor relied on a false negative screening result as a basis for not carrying out further urgent investigation of a patient with unexplained symptoms of post-coital bleeding. Although it was accepted that the laboratory had been negligent in misinterpreting the patient's cervical smear, the court concluded that the doctor had also been negligent in relying totally on the results, particularly in the light of evidence that there could be up to a 20% possibility of a false negative result.

A similar line of reasoning could be raised to argue inappropriate reliance had been placed on a care plan document as a basis for care. This relates to the issue of abrogation of responsibility discussed below.

Liability for miscommunication

Another issue can be described as the 'illusion of communication'. A member of a care team may enter data into the shared information system and assume this is sufficient to draw it to the attention of others on the team. In practice, however, there may be reasons why that data is not viewed and acted upon by others in a sufficiently timely manner. There may be errors in entering data, system error, or design limitations that are insufficiently understood. For example, a team member may assume any new data entered into the system is immediately drawn to the attention of the GP when in fact the system alerts the GP only when he or she next reviews the patient's file.

The available case law on liability for miscommunication relates to issues such as illegibility of handwriting, but it suggests that both parties to the miscommunication may share liability. In one case, a GP was found 25% responsible when a pharmacist misread his script for Amoxil and dispensed a dose some fifty times the permitted daily maximum.[6]

Shared responsibility, abrogation of responsibility

Duties may be inappropriately delegated. Questions may arise about who is responsible for ensuring a patient receives appropriate treatment in accordance with their care plan or that the plan is varied where it is found to be inappropriate.

There is always a danger when several people are involved that they may incorrectly abrogate their duties on the assumption that someone else is responsible. Once again, liability may be allocated between team members if something goes wrong.

It is therefore vital for someone – most logically, the GP – to have overall responsibility and for each team member to have a very clear idea about their specific responsibilities.

Duties of recall and follow up

There seems to some confusion about the standards expected for patient recall and follow-up and how far the duty extends (see Harcourt 2001). Three key Australian cases shed light on this issue.

In 1996, the New South Wales Court of Appeal upheld judgment against a doctor who failed to follow up on a patient's failure to attend an appointment with a gynaecologist to investigate prolonged vaginal bleeding.[7] When the patient's cancer was later discovered, it was too late for a hysterectomy and she required radical radiation, which resulted in serious side effects. The court held that the doctor's failure to refer her to a specialist in another town, when he found that she was unable to make arrangement to travel to Tamworth, constituted negligence. In finding against Dr Kalokerinos, the court accepted evidence by the patient that she would have attended the appointment had she been adequately informed of the potential consequences of not attending. However, the court found the patient was partially responsible for the outcome because she continued to ignore the vaginal bleeding for quite a long period despite knowing that it could be a potential symptom of cancer. Therefore, damages were reduced by 20%.

The South Australian case of *Kite v Malycha*[8] concerned the duty of a surgeon to follow up on a pathology report in relation to a needle biopsy of his patient's breast. The report indicated the specimen was highly suspicious of an underlying carcinoma. However, it was not seen or followed up on by Dr Malycha and Mrs Kite was not followed up when she failed to attend her next appointment. As a result, the cancer had spread to other parts of Mrs Kite's body before the lump was ultimately removed.

The court awarded Mrs Kite and her husband over $500,000 damages and concluded that, on the balance of probabilities, the cancer would either have been cured, or Mrs Kite would have had a much greater life expectancy, had she received appropriate treatment immediately following the biopsy. In finding against Dr Malycha the court commented that he should have recorded the biopsy procedure in his notes and should have made some inquiry to find out what had happened to the report. Furthermore he should at least have become aware of the absent report when Mrs Kite missed her next appointment.

The court did not find any contributory negligence on the part of Mrs Kite due to the failure to counsel her about the potential significance of the test. In reaching this conclusion Justice Perry commented:

> In general terms, Mrs Kite owed a duty to exercise reasonable care for her own safety and well being. But her conduct must be judged in the light of the circumstances as a whole. Dr Malycha concedes that he reassured her as to her condition when she saw him on 2 December 1994. Very likely his reassurance would have led her to believe that a follow-up consultation was not so important as it might otherwise have been. As I have said, irrespective of whether she rang up about it, she was entitled to assume that if the outcome of the testing of the biopsy gave cause for concern, she would be informed. No doubt she would then have sought further advice.

A similar approach was taken by the New South Wales Court of Appeal the following year in *Tai v Hatzistavrou*.[9] In this case, the doctor ordered tests to exclude the possibility of cancer. However, there were delays and errors by hospital staff in arranging the tests. Once again, neither the doctor nor the patient followed up on them. As a consequence, the cancer spread to other parts of her body before a test was ultimately carried out.

The Court of Appeal upheld the decision of the Supreme Court finding Dr Tai liable for negligence. In his judgement, Priestley JA commented that:

> If the doctor thinks it necessary, even for only prudential reasons, that the patient should submit to a particular surgical procedure, then the doctor has a continuing duty to advise the patient to submit to the surgical procedure, so long as the doctor/patient relationship is on foot.

There was no finding of contributory negligence because the patient was not counselled about the need to have the procedure.

To summarise, while each case depended very much on its individual facts, important principles are clear:

1. The key issue is whether the doctor acted reasonably in the circumstances. What is reasonable must take into account the fact that patients do not always do as they are told.
2. There needs to be sufficient communication to ensure that the patient understands what it at stake.
3. What is reasonable will also be affected by the ease with which a follow-up system can be implemented.

An electronic system able to generate reminders can serve a valuable role in avoiding liability for failures to follow up or recall patients. However, there is also a danger that it may create additional expectations and therefore affect the judgment of what is reasonable in the circumstances. In *Kite v Malycha* the fact that a patient expected to be contacted in the event of an adverse report was sufficient to exclude any liability on her part. There may be a danger that patients who are aware that an information system can generate reminders will have a reasonable expectation that this will always occur.

There is also a risk that team members may rely on an information system inappropriately and be liable if a patient suffers adverse consequences because of it. This may be because the system is not designed to generate all of the reminders required or because something goes wrong such as an entry error or some technical problem.

CONCLUSION

A range of important issues need to be resolved when implementing IT-based collaborative treatment models.

Privacy and security are both important. It is essential to implement appropriate technical and procedural security measures and to ensure that patients provide fully informed consent to participation and retain the ability to exercise control over subsequent inputs of information.

It is also vital to manage the risk of negligence claims. This requires appropriate protocols which are reviewed regularly to ensure that they meet current best practice, clear allocation of responsibilities and obligations across a care team, a thorough understanding of what can realistically be expected of such a system, and how it fits in with a patient's overall care. All of this requires time to ensure that each team member fully understands the system and not simply how to operate it. Equally, it requires time with patients to ensure they also have a realistic understanding of it.

ACKNOWLEDGEMENTS

This article is based on a paper presented at the 8th Greek Legal and Medical Conference, Corfu, September 2009.

The CDM-Net project was funded by the Department of Broadband, Communications and the Digital Economy under its Clever Networks program. Project partners are the Victorian Department of Innovation, Industry and Regional Development, Victorian Department of Human Services, Multimedia Victoria, CSIRO e-Health Research Centre, IBM, Intel, Cisco Systems, Global Health, Monash, Deakin and Victoria Universities, Barwon Health, Diabetes Australia (Victoria) and the GP Association of Geelong.

REFERENCES

Department of Broadband, Communications and the Digital Economy (DBCDE). 2011. 'CDM-Net: A Broadband Health Network for Transforming Chronic Disease Management'. Accessed 13 July 2011. Available from: http://www.dbcde.gov.au/digital_economy/programs_and_initiatives/clever_networks/isd/cdm-net_a_broadband_health_network_for_transforming_chronic_disease_management.

CDM-Net Final Report. 2010. Executive Summary 2-3. Available from: http://ebookbrowse.com/cdm-net-final-report-executive-summary-20100520-pdf-d43444117.

Coiera, Enrico; Clarke, Roger. 2004. 'E-Consent: the design and implementation of consumer consent mechanisms in an electronic environment'. *Journal of American Medical Informatics Association* 11 (2): 129-140.

Commonwealth Department of Health and Aging. 'eHealth sites' webpage. Accessed 29 March 2011. Available from: http://www.yourhealth.gov.au/internet/yourhealth/publishing.nsf/Content/eHealth-sites-factsheet.

Dearne, Karen. 2009. 'NEHTA releases strategic plan'. *Australian IT.* Accessed 2 October 2009. Available from: http://www.theaustralian.com.au/australian-it/nehta-releases-strategic-plan/story-e6frgamf-1225782015674.

Evans, Alison; et al. 2008. 'Medicolegal implications of a multidisciplinary approach to cancer care: Consensus recommendations from a national workshop'. *Medical Journal of Australia* 188: 401-404.

Hagan, Kate. 2011. 'Electronic health records planned'. *Age*, 30 March 2011. Available from: http://www.theage.com.au/national/electronic-health-records-planned-20110329-1cexj.html.

Harcourt, Victor. 2001. 'The doctor's duty to follow up: legal fiction, a return to paternalism or an exercise in risk management?' *Journal of Law and Medicine* 8(3): 286-301.

Goss, John. 2008. *Projection of Australian health care expenditure by disease, 2003 to 2033* (AIH, 2008). Available from: http://www.health.gov.au/internet/nhhrc/publishing.nsf/Content/16F7A93D8F578DB4CA2574D7001830E9/$File/Projection%20of%20Australian%20health%20care%20expenditure%20by%20disease.pdf.

Lord, Trevor. 2010. 'E-health – when do we want it? Now'. *Australian Medicine* (June).

Mainsbridge, Anne. 2002. 'Employers and Genetic Information: A New Frontier for Discrimination'. *Macquarie Law Journal* 2: 61.

Medicare Australia. *Medicare Benefits Schedule item statistics reports*. Available from: http://www.medicareaustralia.gov.au/statistics/dyn_mbs/forms/mbs_tab4.shtml.

National E-Health Transition Authority (NEHTA). 2010. *Health Identifiers Service Communications Plan*: 5.

Office of the Federal Privacy Commissioner (OFPC). 2001. Guidelines to the National Privacy Principle: 45 (Tips for compliance with the data security principle).

Paterson, Moira et al. 2011. 'Electronic care plans and medicolegal liability' *Australian Family Physician* 40 (6): 432-434.

Paterson, Moira. 2004. 'HealthConnect and privacy: A policy conundrum'. *Journal of Law and Medicine* 12 (August): 80-90.

Paterson, Moira; Mulligan, Ea. 2003. 'Disclosing health information breaches of confidence, privacy and the notion of the 'treating team''. *Journal of Law and Medicine* 10: 460-469.

Pettigrew, Lisa. 2010. 'A Rising Tide of Expectations'. *HealthVoices* 7 (December): 4-5.

Rivers, Alexandra. 2010. 'eHealth initiatives and Mental Health'. *HealthVoices* 7 (December): 13-15. Available from: https://www.chf.org.au/pdfs/chf/Health_Voices_November_2010.pdf.

Rothe, Ulrike et al. 2008. 'Evaluation of a Diabetes Management System Based on Practice Guidelines, Integrated Care and Continuous Quality Management in a Federal State of Germany'. *Diabetes Care* 31: 863-868.

Roxon, Nicola. 2011. 'Transcript of Press Conference, Melbourne, 29 March 2011'. Available from: http://www.health.gov.au/internet/ministers/publishing.nsf/Content/9815B807A6CF4020CA257862001F3BB3/$File/nr290311.pdf.

Sankar, Pamela; Mora, Susan; Merz, Jon; Jones, Nora. 2003. 'Patient Perspectives of Medical Confidentiality: A Review of the Literature'. *Journal of General Internal Medicine* 18 (8): 659–669.

Terry, Nicolas P; Francis, Leslie P. 2007. 'Ensuring the Privacy and Confidentiality of Electronic Health Records'. *University of Illinois Law Review* (2007): 681-735. Available from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=886904.

Terry, Nicolas. 2004. 'Electronic Health Records: International, Structural and Legal Perspectives'. *Journal of Legal Medicine* 12 (1): 26-39. Available from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1265025#%23.

Win Khin Than. 2005. 'A review of security of electronic health records'. *Health Information Management Journal* 34: 13-18.

Victorian Law Reform Commission (VLRC). 2002. *Workplace Privacy Issues Paper* (2002): xi-xii.

Woodhead, Michael. 2011. 'PCEHR Pledged for July 2012'. (6 April 2011). Available from: http://www.6minutes.com.au/news/pcehr-pledged-for-july-2012.

Zwar, Nicholas et al. 2008. 'Multidisciplinary care plans and diabetes -- benefits for patients with poor glycaemic control'. *Australian Family Physician* 37 (11): 960-962

ENDNOTES

1. The CDM-Net project was funded by the Department of Broadband, Communications and the Digital Economy under its Clever Networks program. Project partners are the Victorian Department of Innovation, Industry and Regional Development, Victorian Department of Human Services, Multimedia Victoria, CSIRO e-Health Research Centre, IBM, Intel, Cisco Systems, Global Health, Monash, Deakin and Victoria Universities, Barwon Health, Diabetes Australia (Victoria) and the GP Association of Geelong. The first author provided legal consultancy services for that project and was a co-author of a chapter on Medico-Legal Studies in the CDM-Net Final Report. The second author managed the research component of the project and was an author and/or co-author of most chapters of the Final Report.

2. *Privacy Act 1988* (Cth); Privacy and Personal Information Protection Act 1998 (NSW); Northern Territory Information Act 2002 (NT); Information Privacy Act 2009 (Qld); Personal Information Protection Act 2004 (Tas); Information Privacy Act 2000 (Vic). The Commonwealth Act applies to Australian Capital Territory government agencies. South Australia has an administrative regime based on a set of IPPs (see http://www.legislation.sa.gov.au/Web/Footer/Privacy/Privacy.aspx. The Information Privacy Bill 2007 (WA) currently remains before the WA Parliament

3. *Health Records (Privacy and Access) Act 1997* (ACT; *Health Records and Information Privacy Act 2002* (NSW); *Health Records Act 2001* (Vic). In relation to the NSW law see Connolly C. 2004. 'Managing patient consent in a multidisciplinary team environment — KJ v Wentworth Area Health Service and its implications for HRIPA'. *Privacy Law and Policy Reporter* 26.

4. *Hookey v Paterno* [2009] VSCA 48.

5. O'Shea v Sullivan and Macquarie Pathology (1992) ATPR (Digest) 46-124; (1994) *Aust Torts Reports* 81-273.

6. *Prendergast v Sam and Dee Ltd, London Times*, 14 March 1989.

7. *Kalokerinos v Burnett*, unreported, NSW Court of Appeal, 30 January 1996. See Gerber, Paul. 1997. 'Kalokerinos Case: More Sinned Against than Sinning?' *Journal of Law and Medicine* 4: 322.

8. *Kite v Malycha* (1998) 71 SASR 321.

9. *Tai v Hatzistavrou* (Unreported, New South Wales Court of Appeal, 25 August 1999) (followed in *Giurelli v Girgis* (1980) 24 SASR 264; (1980) 86 LSJS 25). Devereux, John. 2001. 'Tai v Hatzistravou'. (2001) *Journal of Law and Medicine* 8: 377-378.

Cite this article as: Paterson, Moira; Jones, Kay. 2011. 'IT-based collaborative healthcare initiatives: a legal analysis'. *Telecommunications Journal of Australia* 61 (3): 42.1-42.10. Available from: http://tja.org.au.