

# *Contentious Crop: Harvesting Information from Electronic Health Records*

Written by **Duncan Longstaff** for the Australian National University Faculty of Law Internship Program.

Placement site: Australian Primary Health Care Research Institute, at the Australian National University.

Professional Supervisors: Professor Nicholas Glasgow (Director, Australian Primary Health Care Research Institute); Dr Tom Faunce (Faculty of Law and Faculty of Medicine, Australian National University).

***Abstract:** A major development flowing on from the ongoing conversion of health records to electronic form is the ability to efficiently harvest patient information. This capacity gives rise to a new suite of potential uses for patient health information, as it can now form the basis of meaningful quality assurance and accountability processes, as well as powerful epidemiological studies. However, the fact that medical records can now be readily extracted, transferred and manipulated poses significant risks to data subjects, whose privacy can be compromised by unauthorised access to, and unethical uses of, their health information. Therefore, a balance must be struck between these competing public and private interests to ensure that technology assists society without jeopardising individual privacy. This balance is currently facilitated by duties of confidentiality and statutory privacy rights, but it is becoming increasingly apparent that this framework is not as appropriate for regulating electronic health records as it is for their physical predecessors. The nature and extent of these deficiencies have been brought to light by the recent ‘Camm scam’, which involved a commercial company directly harvesting patient information from record-keeping software for the purposes of selling it on to pharmaceutical companies or anyone else who wished to buy it. Existing legal structures depend upon informed consent, de-identification of data and ethical review, which provide sufficient protection in relation to paper-based records, but may not be able to adequately encompass the issues created by the shift to electronic media. It is important that these fundamental legal issues are resolved before imminent projects such as the Quality and Performance Indicators for Divisions of General Practice and the HealthConnect network come online in the near future.*

## 1. The Promises and Dangers of Electronic Health Records

Computerisation of health records may give rise to a new health care paradigm in which patients, doctors and administrators all have the potential to reap many benefits associated with a rich and sophisticated informational environment. Development of systems able to electronically link, integrate and aggregate individual medical records promises more comprehensive, coordinated and holistic health care for individuals and the community.<sup>1</sup> Perhaps the most significant consequences of adopting electronic media are associated with the ease and efficiency with which patient data can be extracted, transferred and manipulated, features notably absent in paper-based systems, and which could generate a suite of new applications that harness the unique explicative properties of actual patient data, facilitating complex and powerful analyses and providing previously unobtainable insights into individual and population health.

### 1.2 Quality Assurance and Accountability

At the practice level, harvestable patient information offers clear advantages to general practitioners (GPs) and practice managers, who can use it to monitor and evaluate quality of care provided, effectiveness of infrastructure and protocols, and incidences of particular events, such as reportable diseases. Harvesting patient information also holds great potential for informing professional bodies about 'best practice', by revealing unnecessary resource wastages<sup>2</sup> and identifying unexpected side-effects from commonly prescribed pharmaceuticals. Moreover, harvestable patient data can facilitate effective accountability mechanisms in health care; for example, the imminent Quality and Performance Indicators for Divisions of General Practice seek to exploit the elucidatory powers of existing data sets in asthma, diabetes and immunisation registers to measure the effectiveness of individual Divisions in promoting public health through primary care.

### 1.3 Epidemiology

When coupled with the development of infrastructure to link records across numerous data sets, the ability to harvest health information from electronic health records (EHRs) is likely to lead to tremendous advances in epidemiology and public health. Previously, epidemiological studies have been constrained by difficulties associated with data collection; not only because it is enormously laborious and time-consuming, but also

---

<sup>1</sup> Carter M, "Protecting consumers' interests in their health records" (September 1999) 8 *Australian Health Law Bullentin* (2) 13 at 13.

<sup>2</sup> For example, several studies have benefited from the Medic-GP database setup by the University of Adelaide; see Medic-GP: Overview, available @ <http://www.generalpractice.adelaideuni.org/menu/medicgp.shtml>

because data obtained from surveys is typically biased, poorly representative and overly simplistic. Trends and problems in public health are becoming more complex and demand more comprehensive information to understand them.<sup>3</sup> Data generated by linkage of EHRs with, for example, Health Insurance Commission (HIC) data, hospitalisation data and Pharmaceutical Benefits Scheme (PBS) data may provide a comprehensive health care perspective that was previously unattainable; and can be used to monitor the health of a population, identify risk factors and total burden of disease, and determine the effectiveness of treatment or patterns of service usage.<sup>4</sup> Moreover, harvesting data directly from EHRs makes collection quick and cost-effective, reducing the reporting burden on the community and minimising potential biases, particularly regarding sensitive research questions.<sup>5</sup>

#### 1.4 With Benefits Come Risks

Whilst the volume and detail of subject health and personal behaviour will undoubtedly facilitate new and powerful analyses, easy access to and distribution of such detailed health information could also compromise privacy and expose individuals to stress or discriminatory decisions and exploitation in relation employment, superannuation or insurance coverage.<sup>6</sup> With the growing effectiveness of data retrieval engines and ‘data mining’ techniques,<sup>7</sup> once health information is collected in electronic form, it immediately becomes more vulnerable to unauthorized access and exploitation by “data thieves, blackmailers, and others with less than altruistic motives”.<sup>8</sup>

---

<sup>3</sup> Stanley F (2005), *Submission to the Office of the Privacy Commissioner: Respecting Privacy Issues Paper*; document publicly available on the Office of the Privacy Commissioner’s website:

<http://www.privacy.gov.au/act/review/ispap2004.html>.

<sup>4</sup> Bruinsma F, Venn A, Skene L, “Accessing Patients’ Records Without Individual Consent for Epidemiological Research”, (2000) 8 *Journal of Law and Medicine* 76 at 77.

<sup>5</sup> Stanley F (2005), *Submission to the Office of the Privacy Commissioner: Respecting Privacy Issues Paper*; document publicly available on the Office of the Privacy Commissioner’s website:

<http://www.privacy.gov.au/act/review/ispap2004.html>.

<sup>6</sup> Harris RE, “The Need to Know Versus the Right to Know: Privacy of Patient medical Data in an Information-based Society” (1997) 30 *Suffolk University Law Review* 1183 at 1196-1197.

<sup>7</sup> McSherry B, “Ethical issues in HealthConnect’s shared electronic health record system”, (2004) 12 *Journal of Law and Medicine* 60 at 61.

<sup>8</sup> Anderson R, “NHS-Wide Networking and Patient Confidentiality” (1995) 311 *British Medical Journal* 5 at 5.

## 2. The Balancing Act

Whilst the benefits of harvesting health data are largely indirect for individual patients, the possible risks and dangers fall squarely on their shoulders. An appropriate balance must be struck between patient privacy and the interests of other individuals and the broader community in improving public health,<sup>9</sup> but finding an acceptable compromise is inherently difficult. Despite the potential benefits of using harvested data in quality assurance and epidemiological studies, ethical conduct standards clearly dictate that “each research protocol must be designed to ensure that respect for the dignity and well-being of participants takes precedence over the expected benefits to knowledge”.<sup>10</sup> Hence the pivotal consideration is how this data harvesting process impacts on an individual’s interest in their health information, which will vary greatly depending on what information is actually extracted (and in what form), proposed and potential uses of the information, and security measures in place for controlling further access.

With in-house quality assurance or transparent epidemiological studies, where data are harvested and manipulated in an aggregated form, adverse impacts on individuals are relatively minor, and are clearly outweighed by likely benefits to the community. However, in the absence of such a legitimating public interest, it becomes extremely difficult to justify harvesting patient data, no matter how minor the risks to individuals may appear. The informative power of health information makes it a highly valuable commodity, and while a profit motive does not necessarily preclude an activity from being ethical, it is difficult to argue that contributing patients will receive any of the benefits from its commercial exploitation. Therefore, any situations in which health information is harvested for purposes other than quality assurance or public health investigations require close scrutiny.

## 3. A Wake Up Call: The ‘CAMM scam’

A topical illustration of the potential risks of harvesting data for commercial purposes is the ‘CAMM scam’. In 2003, Australia’s leading medical record and prescribing software supplier to GPs, Health Communication Network (HCN), inserted a facility into its ‘Medical Director’ software to enable CAMM Pacific – a company that specialises in monitoring the promotional activities of the pharmaceutical industry<sup>11</sup> – to upload the EHRs of any medical practice where one or more of the doctors in that practice agreed to

---

<sup>9</sup> Patterson M, “HealthConnect and privacy: A policy conundrum” (2004) 12 *Journal of Law and Medicine* 80 at 81.

<sup>10</sup> National Statement on Ethical Conduct in Research Involving Humans (June 1999), Article 1.4

<sup>11</sup> Pollard R, “Cash offer to GPs for information”, *Sydney Morning Herald*, 30<sup>th</sup> October 2004.

participate in its General Practice Research Network (GPRN) in exchange for payment or gift.<sup>12</sup> Only one doctor within each practice needed to assent and activate this facility in order for CAMM to access all records in the practice system, including those of non-participating doctors.<sup>13</sup> Consequently, CAMM could automatically extract the health data of patients at regular intervals, without their individual awareness or consent, and without any external checks or controls over subsequent use of the information. In fact, CAMM has said that the harvested information "...is not just for pharmaceutical companies; it is there for anybody to use – the government, the Health Insurance Commission...we will be selling it to anybody who wants to purchase it".<sup>14</sup>

This entrepreneurial mentality in managing harvested data poses significant risks to patients' interests, which are necessarily subordinated in order to capture the widest possible market to which the information can be sold. Moreover, as trade in health data becomes more established, interested purchasers will demand increasingly detailed and comprehensive information to enable, for example, more complex and powerful actuarial analyses for insurance companies – exposing patients to even greater risks of unwanted disclosure, while failing to benefit or compensate them in any way. Despite these ethical pitfalls in adopting a commercial approach to health data management, both CAMM and HCN refute accusations of any wrongdoing. They claim that data obtained are instantly 'de-identified' – removing all identifying fields except prescription details, gender and age<sup>15</sup> – and that they have no use for patient information because their "...interest is in the prescribing behaviour of the doctor at an aggregated level".<sup>16</sup> They have also stressed that information received from non-contracted doctors is immediately discarded because, not being linked to a particular doctor, it is valueless.<sup>17</sup>

However, it is difficult to be reassured by such claims, because the fact remains that a commercial entity has control of a mechanism to extract comprehensive patient health information without informed consent or limitations on use. Without rigorous external accountability, it is naïve to expect a private company to

---

<sup>12</sup> Limprecht E, "Patient data taken without GPs' consent", *Australian Doctor*, 21<sup>st</sup> January 2005.

<sup>13</sup> Limprecht E, "Patient data taken without GPs' consent", *Australian Doctor*, 21<sup>st</sup> January 2005; see also Limprecht E, "GPs paid peanuts for data", *Australian Doctor*, 10<sup>th</sup> November 2004; and Pollard R, "Computer firm sells GP details for cash", *Sydney Morning Herald*, 21<sup>st</sup> January 2005.

<sup>14</sup> Pollard R, "Cash offer to GPs for information", *Sydney Morning Herald*, 30<sup>th</sup> October 2004 – quoting CAMM Pacific CEO Neil Fox.

<sup>15</sup> Limprecht E, "GPs paid peanuts for data", *Australian Doctor*, 10<sup>th</sup> November 2004.

<sup>16</sup> Pollard R, "Cash offer to GPs for information", *Sydney Morning Herald*, 30<sup>th</sup> October 2004 – quoting CAMM Pacific CEO Neil Fox.

<sup>17</sup> Limprecht E, "Patient data taken without GPs' consent", *Australian Doctor*, 21<sup>st</sup> January 2005 – quoting HCN's Research General Manager Geoff Sayer.

continue to adhere strictly to self-imposed policies on de-identification and data destruction, when they can potentially reap huge profits from selling the more detailed information that they already have exclusive access to. This is not to say that CAMM or HCN are involved (or likely to become involved) in such unscrupulous practices, but the manifest lack of transparency and culpability accompanying their privileged position in itself poses significant threats to patients' information privacy.

There is a clear need for ethical values to be externally imposed on corporations dealing with personal health data, to ensure individual patient interests are protected. However, this runs contrary to the current trend towards private sector deregulation, which prescribes that corporations should be trusted to do the right thing and the market acts as a corrective. The question is how would market forces work here? If patients discovered their GP participated in the 'CAMM scam', and then started transferring to GPs who did not participate, participating GPs would withdraw from the scheme and it would collapse. This is unlikely to happen, because consumers are either consenting or unaware of what is happening, and so market forces cannot work.

Hence, while CAMM and HCN say they are acting ethically and doing all that is necessary to protect patients, this cannot be ensured without external regulation and monitoring. Indeed, a number of key stakeholder groups have already condemned trade in de-identified data as unethical, including the Australian Consumers Association, the General Practice Computing Group, and most recently the Australian Medical Association.<sup>18</sup> Consequently, the efficacy and sufficiency of existing legal and regulatory frameworks in protecting against the possible dangers associated with EHRs is in question. The fact that one of the major risks associated with harvesting electronic health data has already manifested itself as the 'CAMM scam' is of grave concern and it is vital that the capacity of Australia's legal framework to address these issues is critically examined.

#### **4. Electronic Health Information & The Law**

As discussed above, the capacity to harvest health data creates an unbalanced distribution of benefits (which accrue mostly to third parties and the community) and risks (which are borne by the individual subjects of the information being gathered). A consequence of this imbalance is that activities of beneficiaries of harvested data are not necessarily influenced by possible negative consequences, which are unlikely to

---

<sup>18</sup> Limprecht E, "GPs warned over selling patient data", *Australian Doctor*, 23<sup>rd</sup> November 2004; "Data mining: tell patients, says AMA" *Pharma In Focus*, 31 January 2005.

directly affect them. This is just as true of researchers and other parties with ‘legitimate’ public interests, who are often vehement in propounding the importance of their research activities, as it is of profit-minded commercial entities like CAMM and HCN. Hence responsibility ultimately lies with governments to implement and oversee effective legal and regulatory structures that monitor the uses of this technology and ensure that it assists society without compromising the interests of individuals.

#### 4.1 Ownership of Health Information

An important starting point in regulating electronic health information is determining ownership, but the position under Australian law is neither simple nor clear-cut. The landmark case of *Breen v Williams* conclusively upheld the proprietary rights of doctors to medical records created by them, on the basis that “[d]ocuments prepared by a professional person to assist the professional to perform his or her professional duties are not the property of the lay client; they remain the property of the professional”.<sup>19</sup> The High Court also recognised the copyright of doctors in the information they contain, and that the combined effect of these real and intellectual property rights is that doctors are entitled to refuse access to the records, and possess the exclusive right to reproduce them in any material form.<sup>20</sup> Although the contents of the record are ‘about’ the patient, Dawson and Toohey JJ explained that “[t]here can be no proprietorship in information as information because, once imparted by one person to another, it belongs equally to them both”.<sup>21</sup> Hence, the doctor’s proprietary rights in the physical records trumped the supposedly mutual interests in the information itself; implying that priority in information control, as it exists independently of the record, is determined by other factors, such as independent legal rights and competing public and private interests.

#### 4.2 The Duty of Confidentiality

While *Breen* establishes that “[t]here is no innominate common law right of [patient] access to medical records”,<sup>22</sup> it is important that this is not confused with granting doctors an unfettered right to determine who else has access to the information. The circumstance in which medical information is imparted places doctors under an obligation of confidentiality, which protects the rights of individuals to impose restrictions on the

---

<sup>19</sup> *Breen v Williams* (1996) 186 CLR 71, per Brennan CJ; *Duncan v Medical Disiplinary Committee* [1986] 1 NZLR 513; *W v Edgell* [1990] 2 WLR 471.

<sup>20</sup> *Breen v Williams* (1996) 186 CLR 71.

<sup>21</sup> *Breen v Williams* (1996) 186 CLR 71, per Dawson and Toohey JJ.

<sup>22</sup> *Breen v Williams* (1996) 186 CLR 71, per Gaudron and McHugh JJ.

use of secret information by those to whom it is disclosed in confidence.<sup>23</sup> This duty originates from the ancient Hippocratic Oath,<sup>24</sup> with its modern legal basis arising from the fiduciary nature of the doctor-patient relationship, which obliges that the doctor act only in the patient's best interests,<sup>25</sup> and the related equitable action for breach of confidence, which protects patients from actual or threatened unauthorised use of their health information to their detriment.<sup>26</sup> Thus, whilst patients have no property in the contents of their medical records, "...equity acts to protect confidential information, and the degree of protection afforded makes it appropriate to describe it as having a proprietary character...not because property is the basis upon which protection is given...[but rather] because of the effect of that protection".<sup>27</sup> This broad protection provided by the duty of confidentiality can also be further underpinned by the tort of negligence, professional codes of ethics, and the existence of express or implied terms relating to information disclosure in the doctor-patient service contract.<sup>28</sup>

This creates an impasse: doctors are empowered by their proprietary rights to determine whether or not patients can access their health information, yet they are simultaneously constrained in further exercising these exclusive rights of choice over whom the records are disclosed to by their duty of confidentiality. The balance of power therefore lies with the patient, and more specifically in whether or not they consent to the doctor disclosing their health information for purposes beyond the treatment and advice for which it was initially collected.

#### *4.3 The Desirability of Consent as a Fulcrum*

Whilst this focus on patient consent, emanating from the cumulative outcome of *Breen* and duties of confidentiality, accords with intuitive feelings that patients should be in total command of information that reveals so much about them, it may not be as desirable or workable in relation to EHRs as it is with paper-based medical records.

---

<sup>23</sup> Patterson M, Mulligan E, "Disclosing Health Information, Breaches of Confidence, Privacy and the Notion of the 'Treating Team'", (2003) 10 *Journal of Law and Medicine* 460 at 461.

<sup>24</sup> Mendelson D, "Travels of a medical record and the myth of privacy", (2003) 11 *Journal of Law and Medicine* 136 at 139.

<sup>25</sup> Patterson M, Mulligan E, "Disclosing Health Information, Breaches of Confidence, Privacy and the Notion of the 'Treating Team'", (2003) 10 *Journal of Law and Medicine* 460 at 462 – citing *Rogers v Whitaker* (1992) 175 CLR 479.

<sup>26</sup> Patterson M, Mulligan E, "Disclosing Health Information, Breaches of Confidence, Privacy and the Notion of the 'Treating Team'", (2003) 10 *Journal of Law and Medicine* 460 at 465 – citing *Coco v AN Clark (Engineers) Ltd* [1969] RPC 41 at 47.

<sup>27</sup> *Breen v Williams* (1996) 186 CLR 71, per Dawson and Toohey JJ – citing Gummow J in *Smith Kline & French Laboratories (Aust) Ltd v Secretary, Department of Community Services and Health* (1990) 22 FCR 73 at 121.

<sup>28</sup> Mendelson D, "Travels of a medical record and the myth of privacy", (2003) 11 *Journal of Law and Medicine* 136 at 139.

With physical records, centrality of consent in confidentiality appears to strike an appropriate balance between competing interests. There is relatively little for researchers to gain from paper records, due to the sheer impracticability of gathering and collating the data they contain, and so need for consent does not unreasonably obstruct public good. Where public interest is so compelling that it is worthwhile gathering information from individual medical records, the situation can be explained to patients as the need arises, and a vast majority will support the process if it promises genuine benefits without unduly compromising their individual interests.

However, physical records are extremely comprehensive and it is very difficult to effectively limit the fields to which a party is privy once they have been granted access to the record. These practical realities highlight the risk of possible patient detriment and so it is entirely appropriate that individual data subjects should be vested with control over whom the information in their physical records may be disclosed to.

The suitability of this consent-based model for EHRs is more questionable. The ability to readily and effectively harvest electronic health data will facilitate research on quality assurance and epidemiology, with potentially profound consequences for health care delivery. Requiring positive consent for extraction and use of data represents an impediment to such research, which often requires quick and wide-ranging access to health information within patient medical records, and consequently threatens progress in public health. The capacity to harvest electronic health information also alters the relative impacts and risks borne by patients. On one hand, information technology can provide greater protection to data subjects through access control mechanisms, including the ability to selectively mask certain fields of data, such as information regarding abortion, sexually transmitted diseases and drug use. On the other hand, ease of extraction, transfer and dissemination simultaneously makes patient records vulnerable to unauthorised remote access, creating security risks absent in paper-based systems. Thus the situation regarding EHRs is considerably more complex than in relation to paper-based records, as there is a much wider variation between the balance of private and public interests in different scenarios.

From an objective evaluation of competing 'potentials', taking each at its highest value, it seems that the pendulum has swung slightly towards the public interest. It is not so much what patients may lose that has changed, but rather the capacity for those losses to occur; whilst the benefits, have increased in number and variety, as well as likelihood of achievement. Hence the danger is that consent is set apart as the lone indicator of whether an activity should or should not be conducted. In reality, there are numerous additional

factors critical to the evaluation of the overall desirability of extracting and using patient health information, yet which remain unrecognised in the simplistic consent-based model.

#### 4.4 From Confidentiality to Privacy

While confidentiality was traditionally perceived as providing an appropriate protection of patients' interests in their health records, it is becoming clear that "...in a world where the one consumer can be treated by a plethora of practitioners across a diverse range of settings and their records can be electronically mixed and matched with all sorts of other data, [this] traditional approach...is increasingly inadequate".<sup>29</sup> Aside from its inability to recognise the potential for public good created by EHRs, the duty of confidentiality is limited in scope because it only constrains disclosures of information. Patients may not just be concerned about who sees the information, but also how and why it is used. Whilst confidentiality still plays an important role in protecting patients from unwanted dissemination of their health information, it is becoming evident that it fails to address their more general privacy interests.

Privacy is concerned with the scope and limits of personal autonomy,<sup>30</sup> and so is a much wider concept than confidentiality because it "...relates less to interpersonal communications and more to the right to control information about oneself and the right to exclude others from accessing it".<sup>31</sup> Because this 'control' encompasses a much wider range of patient interests, including how information is used and manipulated, in some instances, privacy can be even more restrictive than confidentiality in relation to permitted disclosures. Privacy not only limits disclosure and use in relation to third parties, it also places limits on what doctors and others within confidential relationships can do with the information, meaning that it can potentially constrain not only external epidemiological studies, but even 'in-house' quality assurance processes, if these exceed the limits and expectations of individual data subjects. However, because 'control' is tractable and tailored to actual patient needs and concerns, rather than a rigid requirement of secrecy, in many instances privacy may be less restrictive than confidentiality, due to its ability to account for other important factors, including public interest and the actual risks posed to individual privacy by particular circumstances. It is this

---

<sup>29</sup> Carter M, "Protecting consumers' interests in their health records" (July/August 1999) 6 *Privacy Law and Policy Reporter* 13.

<sup>30</sup> See Mendelson D, "Travels of a medical record and the myth of privacy", (2003) 11 *Journal of Law and Medicine* 136; and McSherry B, "Ethical Issues in HealthConnect's shared electronic health record system" (2004) 12 *Journal of Law and Medicine* 60.

<sup>31</sup> Mendelson D, "Travels of a medical record and the myth of privacy", (2003) 11 *Journal of Law and Medicine* 136 at 140 – citing Ortiz DR, "Privacy, Autonomy and Consent" (1989) 12 *Harvard Journal of Law and Public Policy* 91 at 91-92.

adaptability to the prevailing balance of individual interests and external factors that makes privacy critically important in the context of EHRs.

#### 4.5 Privacy in Australia

Privacy is a universally acknowledged human right,<sup>32</sup> however it was not explicitly recognised under Australian law until relatively recently, with the enactment of the *Privacy Act 1988* (Cth). Increased threats to both confidentiality and privacy resulting from rapid expansion of computerised data systems, particularly in health care, made this publicly-targeted legislative scheme grossly inadequate for protecting individuals in their interactions with the private sector, including GPs and other health care providers. To address these shortcomings, the Australian Government bolstered federal privacy laws through *The Privacy Amendment (Private Sector) Act 2000* (Cth),<sup>33</sup> which extended the operation of the *Privacy Act* to govern collection, storage, usage and disclosure of personal information by organisations, including all health service providers. The essence of this now comprehensive scheme is embodied in ten National Privacy Principles (NPPs),<sup>34</sup> which are largely collection-centric, meaning that, in the absence of consent, identifiable information may only be used or disclosed for the primary purpose for which it was collected, or for directly-related secondary purposes, if the latter fall within the reasonable expectations of the individual.<sup>35</sup>

Throughout the States and Territories there is a patchwork of enactments mandating confidentiality and privacy of health information in specific circumstances,<sup>36</sup> and in some jurisdictions there are dual regimes governing the handling of health records whilst in others there is incomplete coverage, due to a lack of public sector privacy laws in some States. To address this disparity, a National Health Privacy Working Group has been created to develop a national health privacy framework,<sup>37</sup> which, for reasons relating to the realities of effective implementation, as much as Commonwealth parliamentary supremacy, is likely to bring State and Territory regimes into line with federal privacy legislation. Such an approach would also acknowledge the increasing acceptance of NPPs as defining best practice in health information management, which is

---

<sup>32</sup> As reflected in Article 17 of the *International Covenant on Civil and Political Rights*, the English text of which is set out in Schedule 2 to the *Human Rights and Equal Opportunity Commission Act 1986* (Cth).

<sup>33</sup> For the consolidated legislation see [http://www.privacy.gov.au/publications/privacy88\\_030504.pdf](http://www.privacy.gov.au/publications/privacy88_030504.pdf) viewed June 2004.

<sup>34</sup> Contained in Schedule 3 to the amended *Privacy Act 1988* (Cth).

<sup>35</sup> Patterson M, Mulligan E, "Disclosing Health Information, Breaches of Confidence, Privacy and the Notion of the 'Treating Team'", (2003) 10 *Journal of Law and Medicine* 460 at 465

<sup>36</sup> For example: *Health Records (Privacy and Access) Act 1997* (ACT), s 17; *Health Act 1993* (ACT), s 10; *Health Records and Information Privacy Act 2002* (NSW); *Health Records Act 2001* (Vic); *Information Act 2002* (NT).

<sup>37</sup> Paterson M, "HealthConnect and privacy: A policy conundrum", (2004) 12 *Journal of Law and Medicine* 80 at 83; *HealthConnect, Interim Research Report, Vol 1, Overview and Findings* (2003) p 39.

reflected by their incorporation into ethical codes and professional guidelines.<sup>38</sup> Furthermore, unified privacy laws will be crucial to the feasibility of the planned national HealthConnect network of EHRs. With this context in mind, it is pertinent to concentrate on the operation and effect of federal privacy legislation regulation in determining whether Australian law is capable of properly managing the privacy interests of individuals and addressing the issues associated with harvestable electronic patient health information.

#### 4.6 Exceptions, Discretions and Enforcement under the Privacy Act

The default position set up by the *Privacy Act* is a level of protection that renders individual interests pre-eminent by prohibiting any traffic or use of identifiable information without consent.<sup>39</sup> This position is even more restrictive than the duty of confidentiality, and thus it is unsurprising that it is qualified by an array of enumerated exceptions and discretions to accommodate activities with a strong public interest that would otherwise breach the Act. These exceptions are generally designed to ensure that the privacy requirements do not impose radical or unreasonable changes that unduly burden organisations, and also to introduce the elements of flexibility and adaptability, so important in the context of EHRs.

The most significant qualification in relation to EHRs is the so-called ‘medical research’ exception contained in ss 95 and 95A of the *Privacy Act*, which allows the Privacy Commissioner to “...approve guidelines that relate to the collection of health information for the purposes of (a) research, or the compilation or analysis of statistics, relevant to public health or public safety; or (b) the management, funding or monitoring of a health service”.<sup>40</sup> Currently, such guidelines emanate from the National Health and Medical Research Council (NHMRC), who are explicitly mentioned in s 95, and are contained in the *National Statement on Ethical Conduct of Research Involving Humans* 1999 (the National Statement), which is enforced by the Human Research Ethics Committee (HREC). Hence, rather than setting out prescriptive tests for determining when research is justifiable on the basis that the public interest it pursues “would outweigh to a substantial degree”<sup>41</sup> the privacy interests at stake, the Act effectively bestows the HREC with responsibility for overseeing compliance with privacy law.<sup>42</sup> This scheme is designed to recognise the nature of public health

---

<sup>38</sup> For example, the RACGP’s “Handbook for the Management of Health Information in Private Medical Practice” (2002), available at <http://www.racgp.org.au/downloads/pdf/20021014privacy.pdf>; and the Australian Medical Association’s “Privacy Kit”.

<sup>39</sup> See National Privacy Principle 2 “Use and Disclosure”, as contained in Schedule 3 to the amended *Privacy Act 1988* (Cth).

<sup>40</sup> *Privacy Act 1988* (Cth), s 95A(4).

<sup>41</sup> *National Statement on Ethical Conduct of Research Involving Humans* 1999, Part 18; *Privacy Act 1988* (Cth), s 95A.

<sup>42</sup> Gaze B, “Privacy and Research Involving Humans”, (2003) 10 *Journal of Law and Medicine* 410 at 415.

research, where information is collected from (and therefore disclosed by) an organisation that holds it rather than from the individual concerned, meaning that consent may be difficult to obtain.<sup>43</sup>

From one perspective, this scheme makes sense, in that it provides that privacy law defines the minimal ethically acceptable standard for uses and disclosure of personal information.<sup>44</sup> Moreover, it permits case-by-case evaluation of the merits and relative risks of proposed uses of the health information – which vary widely in relation to EHRs – with deference to the experience and expertise of HREC members in relation to medical practice and research methodologies. There are also practical justifications for the arrangement in relation to procedural efficiency, given that a vast majority of public health research already needs HREC approval in order to receive funding – either directly from the NHMRC, or indirectly from universities. Indeed, frequently researchers cannot even access data sets without ethical approval.<sup>45</sup>

However, entrusting the enforcement of privacy law to an ethics committee creates as many hazards as it has advantages. As Beth Gaze points out, “[t]his is the only area of research ethics in which an HREC is asked to supervise compliance with the law, undermining the usual approach that ethics and law deal with different aspects of activity, and that the roles of the ethics committee is to ensure consideration and monitoring of ethical, not legal, standards”.<sup>46</sup> While HREC members will necessarily be very knowledgeable about the scientific and practical aspects of medical research, they may not be conversant with the nuances of legal doctrine. There is also considerable potential for bias – intentional or otherwise – since HREC members, being predominantly doctors and public health officials, may tend to empathise strongly with the public health objectives of researchers.

Whilst the effect of the legislation is that all ‘research’ activities must comply with the National Statement, the only way HREC can ensure privacy compliance is by withholding research funding. This is, therefore, an effective mechanism for preventing publicly-funded research that threatens privacy, but no such instrument exists for preventing private or financially-independent organisations from carrying out such work. Outside of the research exceptions, enforcement of the *Privacy Act* is based on retrospective complaints<sup>47</sup> and there is significant potential for breaches of privacy to occur within the private sector and remain undetected for a

---

<sup>43</sup> Gaze B, “Privacy and Research Involving Humans”, (2003) 10 *Journal of Law and Medicine* 410 at 414; see also *Privacy Amendment (Private Sector) Bill 2000: Second Reading* (Daryl Williams MP).

<sup>44</sup> Gaze B, “Privacy and Research Involving Humans”, (2003) 10 *Journal of Law and Medicine* 410 at 415.

<sup>45</sup> Stanley F (2005), *Submission to the Office of the Privacy Commissioner: Respecting Privacy Issues Paper*; document publicly available on the Office of the Privacy Commissioner’s website: <http://www.privacy.gov.au/act/review/ispap2004.html>.

<sup>46</sup> Gaze B, “Privacy and Research Involving Humans”, (2003) 10 *Journal of Law and Medicine* 410 at 415.

<sup>47</sup> *Privacy Act 1988* (Cth), Division 1.

long time. Data subjects will usually remain unaware of the research activities, and thus unable to complain to the Privacy Commissioner – which is how the ‘CAMM scam’ appears to have avoided detection.

## 5. Threshold Questions

The combination of confidentiality and privacy laws is a complex system that has the potential to offer great protection to individuals’ interests in their health information, yet simultaneously poses great threats. Whether or not the existing regime is able to strike the appropriate balance between protecting individual privacy and realising public benefits from harvestable electronic health information depends upon the answers to several threshold questions.

### 5.1 What is ‘Medical Research’?

Given the latitude created by the *Privacy Act’s* research exemptions, a great deal is contingent upon what constitutes ‘medical research’. According to the Act, “medical research **includes** epidemiological research”,<sup>48</sup> an inclusive definition that is intentionally broad in order to cater for the diversity of important health-related research that exists or may develop in future. The meaning can be at least partially implied from the examples of ‘statistical analysis’, ‘management’, ‘funding’ and ‘monitoring’ enumerated in s 95A, but even these are intentionally vague and imprecise. Similarly, while the ‘health services’ referred to in s 95A(4)(b) are extensively defined by the Act, what is ‘relevant to public health or public safety’ under s 95A(4)(a) is open to interpretation. For example, CAMM could legitimately argue that their activities in harvesting data from Medical Director are ‘relevant to public health and safety’, in that they are providing pharmaceutical companies with information that could potentially be used to detect adverse effects of drugs, as evidenced by fluctuations in prescription rates. The irony here is that, the more privacy is compromised by extraction of increasingly detailed personal information from EHRs, the more useful the data becomes in monitoring effects of pharmaceuticals at the population level, in turn strengthening the argument for exempting the activity as ‘research’. Whether or not this apparent ‘loophole’ could exonerate CAMM and HCN in relation to their data harvesting activities remains to be seen. The imminent publication of the Privacy Commissioner’s report is timely.

---

<sup>48</sup> *Privacy Act 1988* (Cth), s 6 (emphasis added).

### 5.2 What is 'De-identification'?

The *Privacy Act* only restricts the use and disclosure of 'sensitive' information, including "health information **about** an individual"<sup>49</sup> and the current interpretation is that privacy law does not protect information if it is not identifiable, as it is no longer 'about' any individual *per se*. Indeed, the major justification by CAMM and HCN for their activities is that the data they harvest are 'de-identified'. In fact, if the data harvested from Medical Director are capable of being considered no longer 'sensitive' because they are 'de-identified', then CAMM and HCN will no longer have to tenuously rely on the medical research exception, because they will fall under the somewhat peculiar 'direct marketing' exemption in NPP 2.1. Hence a great deal hinges on what effective 'de-identification' entails.

In order to be truly effective, processes of de-identification must render information unable to be identified with particular individuals, making them anonymous. Generally, the larger the data set, the greater the risk of identification;<sup>50</sup> and so it may not be enough that all obvious identifying fields – name, address, birth date, lineage etc – are removed from the record, as there still remains a significant risk, especially in the context of EHRs, for remaining details, such as particular medical conditions, to be linked across data sets. Indeed, even where such details are effectively masked, a sequence of GP consultations over a particular timeframe can often identify an individual if they are linked to a matching sequence of credit card payments, or HIC claims – especially if the party seeking to identify the data is determined and knows who they are looking for. Similar dangers are associated with the use of unique patient identifiers (UPIs), which are coded tags that enable authorised retrieval of encrypted within EHRs, due to the previously delineated difficulties of effectively protecting against data mining. Even where data are aggregated, and no UPIs or identifying fields remain within the EHRs, it will be possible to identify individuals with rare diseases on the basis of geography if each 'cell' or sub-group is relatively small.<sup>51</sup>

Thus it is highly doubtful whether data extracted by CAMM regarding age, gender and prescription information can be described as truly de-identified – but protecting against these possible re-identifications involves trimming patient data to the point where it is no longer useful in epidemiological or quality assurance studies, and so clearly the line must be drawn somewhere. The difficulty is that the potential for

---

<sup>49</sup> *Privacy Act 1988* (Cth), s 6 (emphasis added).

<sup>50</sup> RACGP, "Handbook for the Management of Health Information in Private Medical Practice" (2002), available at <http://www.racgp.org.au/downloads/pdf/20021014privacy.pdf>

<sup>51</sup> RACGP's "Handbook for the Management of Health Information in Private Medical Practice" (2002), available at <http://www.racgp.org.au/downloads/pdf/20021014privacy.pdf>

re-identification will be highly context-dependent, in that while a particular field could easily lead to re-identification in some instances, the risks are significantly less in others. Hence, whilst de-identification has great potential for simultaneously attending to individual privacy interests whilst enabling use of data for public interest purposes, its parameters must be explicitly defined, in a study-specific manner, as opposed to a simple blanket catch-phrase that data are ‘de-identified’.

### 5.3 What is ‘Informed Consent’?

The relative desirability of consent as a fulcrum for confidentiality and privacy has already been discussed. Nevertheless, it is firmly entrenched in the law surrounding uses and disclosures of health information, and a large proportion of the *Privacy Act* is devoted to finding ways to justify its absence. Given this potential for ‘informed consent’ to completely obviate the difficulties surrounding privacy exemptions outlined in this discussion, it is important to appreciate what it actually means.

Consent refers to “...a patient’s informed and voluntary agreement to confide or permit access to or the collection, use or disclosure of his or her health information for specific purposes”.<sup>52</sup> The *Privacy Act* provides that consent may either be express, or implied from the action or inaction of the individual. An important part of consent is the patient’s ability to tailor its scope and content, and so the individual “...must know what it is he or she is agreeing to and be aware of the implications of providing or withholding consent”.<sup>53</sup> The *Privacy Act* establishes a system where consent is obtained at the point of collection, which is aimed at making it practically possible to obtain consent from all patients, which would otherwise be very difficult to do post-consultation. However, ‘up-front’ consent presents difficulties, because it will be impossible for either doctor or patient to foresee all potential uses of the information, especially given the rapid proliferation of epidemiological studies already occurring as a result of the emergence of EHRs. As well as these unforeseeable uses, there are more immediate difficulties with implying consent, “...as the patient may assume that the information is being provided exclusively for treatment of a specific condition or problem rather than for a broader, more holistic purpose”.<sup>54</sup> Moreover, a patient may implicitly consent to

---

<sup>52</sup> Canadian Medical Association, Health Information Privacy Code (15 August 1998), Section B, Definitions – cited in McSherry B, “Ethical issues in HealthConnect’s shared electronic health record system”, (2004) 12 *Journal of Law and Medicine* 60 at 64.

<sup>53</sup> Patterson M, Mulligan E, “Disclosing Health Information, Breaches of Confidence, Privacy and the Notion of the ‘Treating Team’”, (2003) 10 *Journal of Law and Medicine* 460 at 469.

<sup>54</sup> Patterson M, Mulligan E, “Disclosing Health Information, Breaches of Confidence, Privacy and the Notion of the ‘Treating Team’”, (2003) 10 *Journal of Law and Medicine* 460 at 465.

disclosures and uses of their data by other health care providers, but not third parties who are not involved in their treatment, a distinction which the doctor may fail to recognise.<sup>55</sup>

Given these difficulties in getting up-front consent that is both comprehensive and meaningful, and the impossible burden of obtaining real-time consent from every data subject as and when their information is harvested for use in a study, a great deal of significance falls on the default position of the Act: in the absence of consent, information may only be used or disclosed for the primary purpose for which it was collected, or for directly related secondary purposes if the latter fall within the reasonable expectations of the individual. Yet even this has the potential to cause controversy in relation to what are 'reasonable expectations'. Doctors are likely to impose their own perceptions of what is reasonably expected by patients, which may or may not be consistent with patient expectations.

Another concern is that 'informed consent' under the *Privacy Act* is not consistent with current 'best practice'. Whereas the *Privacy Act* stipulates that patient consent is not required for use of de-identified data, 'best practice' requires patients be informed of **any** proposed disclosure to third parties.<sup>56</sup> Consequently, doctors are effectively given a choice of whether to ignore 'best practice' and 'keep their mouths shut' in order to take advantage of the de-identified data exceptions in the *Privacy Act*, or risk foregoing the advantages of harvesting information by going through a lengthy explanation to each of their patients of the many possible ways in which their data **might** be used in order to obtain tailored consent.

## 6. The Future

The existing legal framework surrounding use and disclosure of electronic health information is built upon three pillars: informed consent, de-identification and ethical review. In effect, these components form a cascade, in which patient consent remains the central component, but can be circumvented in situations where the data are deemed de-identified. The considerable grey areas regarding when relevant consent exists and when data are sufficiently de-identified to bypass it are largely addressed by the ethical review component of the *Privacy Act*, which allows for informed case-by-case evaluation in order to rationalise the complex balance of competing interests regarding EHRs. However, ethical committees are prone to public biases, and do not provide an effective filter for unscrupulous activities by independently-funded entities not

---

<sup>55</sup> McSherry B, "Ethical issues in HealthConnect's shared electronic health record system", (2004) 12 *Journal of Law and Medicine* 60 at 64.

<sup>56</sup> RACGP's "Handbook for the Management of Health Information in Private Medical Practice" (2002), available at <http://www.racgp.org.au/downloads/pdf/20021014privacy.pdf>

required to undergo ethical review. It is this lack of a private-sector regulatory mechanism where the legal framework falls down. HCN and CAMM are in a uniquely privileged position to exploit this 'loophole', as they have a virtual monopoly over the software through which EHRs are currently created. Assuming they are appropriately reprimanded, and their activities stopped, it is difficult to see how another organisation without such a monopoly could effectively gain access to patient data and simultaneously evade ethical review – but then again, the 'CAMM scam' was not foreseen either. The 'CAMM scam' has served as a clarion call and should be used as a catalyst for debate on how privacy regulation needs to adapt in order to effectively protect individual interests, while maintaining a balance that facilitates use of the data for public good.

The simplest approach is to address the deficiencies of ethical review, firstly by ensuring that HREC and other committees are appropriately balanced by consumer representation, and equipped with legal as well as medical expertise. More difficult is ensuring that review processes extend to privately- as well as publicly-funded activities. This could be achieved by establishing a neutral third party 'trustee', through which all outgoing patient data from a practice must pass, with a properly-constituted ethical committee determining whether or not proposed recipients of the information will use it without breaching the privacy of individual data subjects, and grant or withhold access accordingly. Admittedly, such a comprehensive and centralised database creates a virtual 'honey pot' for hackers, and so a great deal of responsibility will fall upon authentication and security-enabling technologies to ensure system integrity. However, these technologies are already under development in preparation for the launch of the *HealthConnect* network, and the data trustee could be rendered even more ubiquitous if it forms part of *HealthConnect's* infrastructure.

Overall, it appears that existing legal structures regarding health information cannot adequately encompass the issues created by EHRs. Reform is inevitable, but must be done relatively quickly with large projects like the Quality and Performance Indicators for Divisions of General Practice and *HealthConnect* going online in the next few years and creating a swathe of new public benefits and privacy risks. The 'CAMM scam' is a relatively benign reminder of the potential for both patients and doctors to unconsciously lose control over electronic health information – let us hope that the lesson is heeded.