Will the new Australian Health Privacy Law provide adequate protection?

DAVID BOMBA AND GEORGE HALLIT

David Bomba is a Lecturer and George Hallit is a Research Assistant in
The School of Information Technology and Computer Science, University of Wollongong.

Abstract

Amendments to the original Privacy Act (1988) come at a key point in time, as a national medical record system looms on the Australian horizon. Changes to The Privacy Act have the potential to define a level of information privacy prior to the implementation of such a system. We have therefore collected expert opinions on the ability of the Health Privacy Guidelines (enacted in December 2001 under The Privacy Act and hereafter more specifically known as Health Privacy Legislation) to ensure the privacy and security of patient information. We conclude that the legislation is flawed in its capacity to withstand an increasingly corporatised health sector. Deficiencies in consent requirements, together with feeble enforcement capabilities, mean The Legislation cannot effectively ensure that personally identifiable information will not end up in corporate third party hands. To significantly bolster the new legislation, we argue that it should be supplemented with explicit health data legislation and privacy auditing.

Privacy protection in Australia

Privacy is a very subjective concept, and so the boundaries between public and private will always be in dispute. One thing is certain; society's ever-increasing dependence on technology has seen this boundary change. The proliferation of computer use has resulted in massive amounts of personal information being recorded and stored.

As computing power has improved, so too has the ability to process this information. Techniques such as profiling have meant that previously disparate sets of information can be matched, resulting in very detailed profiles of individuals. This personal information has become increasingly valuable to governments and corporations alike. The evolutionary result is that industrialised economies are increasingly becoming more information-orientated. Consequently, organisations have a desire to know and control more about the people they serve, or the clients they deal with. Some authors argue that such organisational behaviour can be seen as indicative of a growing surveillance and control society (Lyon 2001).

To date, Australia has had great disparity between privacy law in the public and private sector. In a concerted effort to rectify this problem, the Privacy Commissioner has published three sets of draft guidelines, effectively broadening the scope of the Privacy Act (1988) to cover the private sector. As one of the three sets of guidelines, the basis for specific health privacy legislation (enacted in December 2001 under The Privacy Act), the Draft Health Privacy Guidelines are specific to the healthcare sector. This finally brings Australia more in line with international attitudes and legislative stances.

Traditionally, as confirmed in the landmark case of Breen v Williams (1994), a patient has no access and ownership rights to the information kept about them by a health provider. In what represents legislative revolution, the Health Privacy Guidelines present Australians with a more open access model. In this way, patients will be able to access, correct, and possibly remove health information stored about them. With the implementation of a national medical record system looming, the Health Privacy Guidelines come at a key point in time. That is, they have the potential to define a level of information privacy prior to the implementation of such a system. Given this potential significance, an assessment of the Guidelines has been of paramount importance.

Since their introduction in May 2001, we have assessed the ability of the Draft Health Privacy Guidelines to ensure patient information privacy and security. The Guidelines proposed considerable change to practitioner information handling practices, and the Privacy Commissioner subsequently faced criticism over what some regarded as a hindrance to proper health care. The amended set of Guidelines was released in October 2001, named Guidelines on Privacy in the Private Health Sector. While these Guidelines still propose a considerable cultural and generational change as to what private sector health providers can do in dealing with health information, they also represent a backdown in stringency from the initial Draft set of Guidelines. Perhaps in response to outcries from practitioner representative bodies, the proposed consent requirements are now less rigid, only adding to the concerns of privacy advocates.

Method: a discussion with experts

We decided to explore a range of issues dealing with The Health Privacy Guidelines among a group of experts through a convenience sample taken in 2001. The exploratory interviews were informal in nature and were primarily conducted to ascertain stakeholder reactions. Representatives from the private health service, patients and government were targeted. After ethics clearance was gained, seven experts in their areas were approached to be interviewed. One person declined and six accepted – of which five were interviewed in person and one over the telephone.

The participants were well versed in their related areas as well as The Draft Health Privacy Guidelines. The sample included a member on the New South Wales Privacy Advisory Committee, a former Chief Information Officer for a New Zealand Regional Health Authority and Concord Hospital in Sydney, The Deputy Chair of the Australian Health Ethics Committee on the National Health and Medical Research Council and contributor to drafting the Guidelines Under Section 95A of the Privacy Act, a research manager involved in developing Smart IDs in conjunction with The Illawarra Division of General Practitioners, The Head of Rheumatology research at Sydney's Royal Prince Alfred Hospital and a pharmacist.

What did the experts have to say?

Interview respondents were asked whether they agreed to the notion that society had become more suspicious concerning threats to their information privacy. All agreed to a rising general level of suspicion. One respondent, herself a privacy advocate, believes this is largely due to the media inflaming matters. Putting the doubt in perspective, another respondent alluded to the flaws of the current, paper-based medical filing system. In the existing system it is quite common for medical records to go missing. However, more often that not it is the case of doctors taking records to peruse at home and misplacing them there. In addition, hospital patient records are kept at the foot of beds, potentially at the mercy of any passer by.

Also placing the public concern in perspective, another expert respondent referred to a growing acceptance of circulating personal information, but spoke of varying levels of trust. That is, people generally accept personal information is required to be 'out there', but certain groups are more trustworthy than others, such as banks and insurers over marketing firms. Indeed, while it may only require a small minority to stir negative media, rises in information surveillance type activity (e.g. data profiling and matching) only serve to validate societal concern.

Whether this lack of trust is on the rise is perhaps a matter for further study, either way it still exists. This suspicion may be underplayed when considering the lack of privacy under manual paper-based systems, but the fact remains: public concern is increasing on the back of ever augmenting computing power. What was previously an arduous task of collecting and reviewing disparate sets of personal information is now more easily facilitated by the growth of computing, data matching and profiling. This improved ability to survey has seen the seriousness and scale of privacy breaches intensify.

The corporatisation of general practice

It could be argued that the healthcare sector in Australia is one of the slowest to adopt information technology, not in regards to medical research, but relating to administrative and clinical practices. One expert respondent supported this stance by further mentioning a reluctance of older practitioners to adopt administrative and

clinical related information technology. Those doctors nearing retirement, comfortable in their private practice, may shy from adopting technology that will fundamentally alter the way in which they create, maintain and store medical records, as well as generate prescriptions. Another respondent referred to the age-old notion of time being equal to money. Any change in practice that would increase the average consultation time for a patient would mean fewer patients consulted per day, and therefore make for less income. It would then follow that practitioners would oppose any changes that would make consultation times longer.

Traditionally, doctors have had a vested interest in protecting patient privacy. Without a trusting patient-doctor relationship, a patient may not reveal all the information required for proper diagnosis and subsequent treatment. The Hippocratic Oath and the maintenance of such a trusting relationship have therefore been central to general practice. Of course, this is insufficient in the electronic and corporate era, where economies give great value to information.

A common belief of respondents pertaining to the medical field is that there appears to be a growing trend for practitioners to enter private 'medical centre' style operations. In such scenarios, organisations or partnerships, usually of medical background, establish multifunctional medical centres. Running a number of health-related businesses, these centres might incorporate a general practice, pathology, x-ray facility, and pharmacy. The centres create secondary flow-on business for involved parties, minimise overhead costs, and give flexibility to practitioners who might otherwise be operating their own practice. In this way, the centres are increasingly commercially attractive. This raises issues in regards to the privacy and security of health information. In the past, partial records would have been distributed between various health service providers in independent locations.

With many operational units now under one roof, the more commercial style operations can potentially generate masses of health information, painting quite a detailed picture of an individual's health. This information's corresponding value to research, marketers, drug companies and insurers alike, would be enormous. Of particular concern, persons with medical backgrounds do not always manage these operations. Being business-minded, the management's propensity to abide by legislation is therefore always under tension. This blurs the boundaries between public health interests and corporate or commercial interests, creating little assurance for patients over who is accessing their health information, and for what purpose. Playing down this concern, one respondent pointed to the high risks involved in on-selling health information. A single complaint under the new legislation could potentially mean the end of that health provider's operations.

In the case of an organisation operating multiple corporate-style centres, the entire chain could be closed or in the case of smaller private operations, the practice itself. For example, even if desperate for funds, a naturopath in private practice may not necessarily generate sufficient health information to arouse market interest. If that naturopath were accredited by the corresponding representative body, and were therefore subsidised by the government, their ethical and commercial inclination to profit from such behaviour would probably be lower.

It appears that while larger organisations will have an abundance of health information, the associated risks with on-selling it would be too great and smaller private sector health providers may not generate sufficient information to justify market interest. The prospect of being put out of business stemming from a single complaint may be sufficient to dissuade any health provider from breaching the new legislation. Other experts seem similarly satisfied with the Guidelines ability to dissuade potential lawbreakers. Nevertheless, in the words of Dr Trevor Mudge, vice-president of the Australian Medical Association (AMA): "there's nothing in this legislation we've seen that will adequately prevent corporate companies from on-selling patients' private medical information for commercial purposes" (Mudge 2001: 9).

While the comments of Dr Mudge may seem a little harsh, one has to keep in mind the differing agendas at play. One expert interviewed warily considers doctors advocating privacy, claiming they are merely disguising their own interests. Certainly, time, and the regulatory change it has brought, has eroded the independence of practitioners.

The introduction of Medicare has seen general practice scrutinised, as governments curtail payments and monitor consultation times. Furthermore, this new legislation is hardly doctor-friendly. In empowering patients with new legal rights, the Guidelines are making practitioners far more accountable for their information management practices.

This increased responsibility carries with it onerous procedures. The Guidelines can be seen as over-prescriptive. Despite claiming to "explain how the NPPs [National Privacy Principles] apply in practice" (OFPC (A) 2001:

14), the Guidelines seemingly attempt to regulate the practice of medicine. According to the AMA, the Guidelines supersede "well-developed principles of clinical and ethical practice that have been the subject of proper processes of public scrutiny" (AMA 2001: 9). As such, they are prescribing how practitioners should deal with their patients, including the manner in which they communicate, and the limitation of what histories are appropriate to be taken (AMA 2001: 10). According to the AMA, "placing privacy above best clinical practice endangers patient health and well being and is ethically unacceptable" (AMA 2001: 10).

Returning to the comments of Dr Trevor Mudge, there may well be genuine cause for concern in the area of on-selling health information. The Privacy Commissioner would surely have insufficient resources to deal with potential privacy breaches to e-health records, "the push to make profits in GP's practices bought by corporate interests raises the risk of inappropriate 'data-mining' of personal data for commercial purposes. The potential insecurity of information held on-line and the speed with which it may be disseminated are real causes for concern" (AMA 2001: 44).

Adjusting to change in information practices within the private healthcare sector

Whether it is positive or negative, the proposed privacy legislation will have a considerable impact on the current practices of private sector healthcare. As one interviewed expert sees it, the new legislation will implement a cultural and generational change over what organisations can do regarding health information.

Perhaps the worst hit area of health is pathology, whose operations are based on the collection and study of patient specimens. The organisational change will be wide-ranging, incorporating changes to the practices of collection, obtaining consent for primary and secondary purposes, as well as the destroying of samples no longer in use. It therefore comes as no surprise that the Royal College of Pathologists of Australasia are requesting a moratorium from prosecution, "as the systems described in these guidelines are going to take some time for organisations to be able to implement them" (Graves 2001: 5).

Similarly, another interviewed expert discussed the problem by using a university setting as an example. In an organisation such as a university, there exists a mass of personal information spread across multiple departments, nooks and crannies. If a student were to request a copy of information held about them, retrieving administrative information would not pose a problem, but as for the remainder, it would pose a mammoth task. The same can be said of hospitals that face similar difficulties in compliance.

One expert pointed to the first review of The Guidelines as being after two years. Considering the impact on organisational practices, a shorter review period would have been preferable. It was suggested that a more realistic six to twelve month initial review be implemented. This was subsequently agreed by other experts interviewed.

The overlapping of public and private spheres

With the proposed Health Privacy Guidelines aimed solely at the private sector, information handling practices of the public and private sectors will be subject to somewhat differing regulations. One respondent points to the inherent confusion this may cause, for private patients in public healthcare, and for privately contracted practitioners in the public sector. However, one expert practitioner interviewed said he saw little problem in adjusting, as there are already stringent practices in place.

One expert respondent, a pharmacist, referred to government desire for greater control over Australian health expenditure. For example, the Australian 'Getting Connected' project creates electronic linkages between the Health Insurance Commission, medical practitioners and pharmacists. While the original promise was to minimise adverse events arising from inappropriate prescribing, the project's major function has been electronic checking of consumer entitlements to medications at concession rates (see Carter 2000: 29).

Medicare was similarly used to empower governments. In scrutinising practitioners, the government has managed to gain greater control over payments and monitor consultation frequencies. In the United States, similar Guidelines have been legislated in May 2001 but are loophole ridden (McMenamin, 2001: 62; Conlan, 2001: 63; Mitchell, 2001: 68; Hoffmann, 2001: 6). Their new ability for government officials to access personal health information without consent is perhaps a reflection of a greater desire for government control. The Australian Health Privacy Guidelines are no different.

It has been mentioned that the Guidelines are somewhat over-prescriptive. Despite setting out to advise on how the NPPs apply in practice, they essentially regulate privacy in the health care sector. Regulation can be seen as the equivalent of control. The interviewed experts generally see the introduction of a universal patient identifier, and a national system for electronic medical records, as a highly likely prospect.

One expert stressed that such a system would have to be introduced subtly. Given the failure of the 'Australia Card', the government may choose not to incorporate the use of a smart card. In addition, the term 'unique identifier' would have to be avoided, even though they already exist, and that one would have to be used. Perhaps The Health Privacy Guidelines represent a move to establish a level of control prior to such a system's implementation. Certainly, The Guidelines propose the imposition of a regulatory framework governing the health care sector, but whether this would effectively enable healthcare's pecuniary supervision would remain to be seen.

Privacy awareness among patients

It could be argued that the public in general is unaware of the vast and all-encompassing level of surveillance taking place. As more of our every day activities are surveyed, the level of public privacy has correspondingly declined. This is juxtaposed alongside technologies that are more blatant in their obtrusiveness. For instance, despite public outrage over the proposed 'Australia Card', the Tax File Number (TFN) was subsequently improved and used to similar effect. Given its more subtle improvements to surveillance power, the TFN faced little, if any such outcry.

While citizens may not be completely aware of the many intrusions to their privacy, the findings of Bomba and de Silva (2001) and the Privacy Commissioner (OFPC (B) 2001) would point to an increased social value and concern over privacy. In particular, society is wary of new surveillance technologies, and values the makers' attention to privacy and security matters. Perhaps society's acceptance of a general level of intrusiveness lies in blind trust, or as a trade off for the goods and services they need and desire. Moreover, perhaps the trust lies in the belief that legislation is in place to prevent and/or prosecute privacy breaches.

This would fit with the Privacy Commissioner's recent findings, where respondents were tested on their knowledge of existing privacy laws. Of the three legislation-related true-false statements, just seven percent (7%) answered all correctly (OFPC (B) 2001: 28). Of more concern, sixty four percent (64%) gave correct answers to less than two statements (OFPC (B) 2001: 28). This trust adds to the significance of having health privacy guidelines. The public should be able to feel secure in the knowledge that overarching legislation is in place, thereby protecting their health information from possible privacy breaches.

Patient willingness to disclose sensitive information

The public has increased its awareness of invasions to their privacy, thereby attributing it with significant value. In a proposal to the experts interviewed, a suggestion was made that patients might be less likely to relinquish sensitive information in consultations, possibly impeding proper care. In this way, a person might be concerned that if they surrender certain sensitive personal information, it may adversely affect them in the future. The proposition was faced with a general air of indifference. The collective opinion being that the majority of the public would have no problem in disclosing necessary information.

However, this has potential impacts on the proper delivery of care. In an example given by the AMA (2001: 27), a patient visits a doctor for inoculation against the flu, choosing not to reveal they are undergoing treatment for AIDS. After all, the Draft Guidelines state that a patient is not required to disclose health information outside the scope of the treatment being sought (OFPC (A) 2001: 35). Relieved that they do not need to disclose this sensitive information, the patient would be likely to die following the interaction of AIDS medication and flu shot (AMA 2001: 27).

Perhaps, as one expert suggests, those persons withholding information might be limited to a minority whose health information may instigate discrimination (e.g. HIV). However, the proportion of people withholding information could potentially explode into a majority. If legislation such as the Health Privacy Guidelines cannot ensure the privacy and security of health information, breaches of privacy will continue to occur. This can lead to a loss of faith in the systems that store and transmit their personal health information. Since it is these technologies that organisations rely upon for administrative and clinical processes, such as pre-

employment background checks, an increased number of people might choose to withhold certain information. While this might prevent them from possible discrimination, it can only be potentially harmful to their health.

The introduction of a national integrated electronic health record system seems likely. Prior to its arrival, it is paramount that legislation be in place that defines our privacy rights, and deters potential offenders by prosecuting those that do offend. If the Health Privacy Guidelines cannot successfully ensure the privacy and security of patient health information, breaches of privacy will only increase. This will lead to more chilling effects of information error, and further people being discriminated against. It therefore follows that an increasing amount of people would choose to withhold health information that could potentially be used against them, thus jeopardising their health.

It was the expectation of the Privacy Commissioner to establish a common-sense framework that balanced the right of individuals to control their information, with the need not to create undue burdens upon health practitioners. Upon reviewing the Draft Health Privacy Guidelines and interviewing the expert group, the following should be considered carefully.

The consent requirements laid down in the Guidelines represent a strong stance taken by the Privacy Commissioner. In the opinion of the AMA, this would interfere in the provision of care, and undermine the primacy of the doctor-patient relationship (AMA 2001: 4). Whether the Guidelines would have such an impact is out of the scope of this paper. However, in requesting more freedom from the Privacy Commissioner, it appears practitioners view matters in terms of confidentiality, not privacy.

One expert agreed and referred to the doctor-patient relationship: to a practitioner, privacy legislation interferes with this relationship, undermines patient trust, and places obstacles in the provision of care. Nevertheless, the Guidelines' recognition of privacy should be welcomed. Even so, the implementation of a more considerate framework might have been preferred, one that acknowledged the sensitivity of the practitioner-patient relationship. An answer may lie in explicit legislation on health data, stating exactly who is entitled to what information. In this way, practitioners might be legally permitted to consult with other practitioners as they currently do, all without requiring consent, as is necessitated under The Guidelines.

Collecting necessary health information from patients

The Guidelines on Privacy in the Private Health Sector state that information collected by a health provider in providing a service should only be necessary information (OFPC (C) 2001: 1). In this way, the Privacy Commissioner is suggesting practitioners only collect information that is appropriate to the scope of the health service requested. This seemingly reasonable requirement has implications on patient privacy.

Aware that consent would have to be sought for information collected for secondary purposes, practitioners may be inclined to seek extra information under the fallacy of being applicable to the health service being sought. For, it appears that under the Guidelines: "the collection of information for secondary purposes is acceptable providing it is contemplated when the original consent was given. However, the precise use that the health provider may wish to make of the information may not be known until some time after the consent is obtained" (Berg & Davis 2001: 3).

One interviewed expert indicated to this grey area with an example, questioning whether a body piercer needs to know if their client has a haematological condition (for example HIV or hepatitis). With increases in general practice computer use, inputting such additional information may become as simple as an extra mouse click. The boundary between primary and secondary purpose could therefore be stretched, resulting in information being disclosed that is outside the scope of providing the health service.

A likely solution lies in explicit legislation on health data, stating exactly who is entitled to what information. With the growth of computing in administrative and clinical health care, the boundary between primary and secondary purpose will only stretch. An advantage of explicit legislation has already been mentioned concerning obtaining consent. In regards to health information collection, explicit legislation is essential in avoiding this exploitation of poorly defined boundaries in legislation.

Use and diffusion of personal information

It is accepted that the disclosure and use of personal information is necessary for health providers to provide adequate care and for possible benefits to accrue in the collection of information for research and statistics. However, concern arises when a health provider discontinues operations. With the value attributed to health information, and the consequent reluctance to destroy it, there exists a massive amount of health information in databases nation-wide.

If for example the owner operator of a general practice dies, or a health provider is taken over by a corporate entity, questions arise as to what happens to the health information involved. According to the Law Reform Commission of Western Australia, the Guidelines "[do] not give sufficient guidance on the application of the NPPs in the context of the corporate development of the health sector" (Kay 2001: 1).

Regrettably, the Guidelines do little to stress the importance of obtaining consent in these situations. That is, where changes in management occur, the Guidelines suggest that it would be "good privacy practice" to notify individuals (OFPC (A) 2001: 90). However, this is described a little differently in the amended Guidelines. Nevertheless, this is still a problematic issue. The idea that individuals might not learn that their sensitive information has changed hands is sure to have its repercussions. For instance, an HIV sufferer may have trusted their local doctor with this sensitive information. However, if this doctor was to move on, and their general practice comes under new management, surely the patient should learn of this addition to their 'circle of confidentiality'.

In this increasingly corporate era, consumers must be assured that legislation prevents their sensitive information from being transferred into commercial hands. In this way, they must first be notified of any change in hands. Also related to the use and disclosure of health information is the issue of patients withholding necessary information. As previously discussed, a growing trend of information entering corporate hands may dissuade patients from exposing their sensitive health information. Unfortunately, this concern would only be fuelled if, under the new Guidelines, consumers were not to be notified of changes to the management of their sensitive information.

Open information management and secure storage and handling

The Guidelines' requirement that an organisation is to be open about its information handling practices is a welcome move. In fact, this openness, as well as the ability to correct one's own information, finally provides the Australian public with a more open access ideal. As has already been mentioned, the ability to access one's own personal information, to remove it, and to correct it if it is wrong, is a good privacy safeguard. Evidence would suggest that such an open model would have a positive effect on the doctor-patient relationship (Carter 1998: 597). However, The Guidelines will impart such a considerable change to current practices that this would have to be seen and evaluated over time.

Benefits aside, The Guidelines only enable consumers to request information. That is, information could be circulating, and even adversely affecting them, without their knowledge. Ideally, the legislation might have required organisations to notify patients that personally identifiable information was held about them. That way, the public could feel secure in that they knew of all their information 'out there', and that it was correct. However, the potential private sector outcry over enormous costs can undoubtedly already be heard.

The Guidelines stipulate that organisations take "reasonable" steps to protect individuals' health information from misuse, loss, or unauthorised access, modification and disclosure. It is also stated that the securing of health information "...reflects a very high standard of security" (OFPC (A) 2001: 69). However, in the subsequent amended Guidelines the wording implies less stringent measures. Possibly, this may have been as a result of the implications of further investment in security technologies in order to produce a very high standard of security.

The national director of intellectual property at Deloitte Touche Tohmatsu, Ulysses Chioatto, claims that some "companies may be forced to re-engineer the technology underpinning their business" (Brown 2001: 21). While this would make for a better privacy safeguard, the costs are sure to be passed on to consumers. Of all experts questioned on this topic, all agreed patients would ultimately foot the bill.

How will privacy legislation be enforced?

Any legislation that relies solely on complaints before investigating possible offenders does give cause for concern. In an era where both developed and developing economies are increasingly becoming more information reliant with computer networks enabling the wider dissemination of information, this approach to legislation is hardly adequate.

The enforcement of the Draft Health Privacy Guidelines is essentially a complaints-driven process. Once legislated as part of improvements to the Privacy Act (1988), individuals will have the right to complain to the Privacy Commissioner if they believe an organisation has breached their privacy rights (OFPC (C) 2001: ii). Unfortunately, the subject of a privacy breach, and the chilling effect of personal information error, is not often realised by the patient until after it has occurred i.e. the damage may have already been done.

In a growing information society, where information exchange is common practice, the likelihood of realising one has had their privacy violated is difficult. Under the new legislation, one interviewed expert pointed out that compensation might be sought for successful complaints. This is also the view of other commentators (see Brown 2001: 21; Stock 2001: 3).

While other experts speak of having operations shut down, legally speaking little can be predicted of the Privacy Commissioner's possible actions, especially since there are no precedents. What is probable is that offenders, if caught, will be taken to the Federal Magistrates Court, where a fine may be issued and their reputation damaged (Brown 2001: 21). In the opinion of two experts interviewed, this would appear to be a sufficient dissuasion. However, for a large corporation seeking to satisfy its profit hungry stakeholders, one can see the tension that arises. Moreover, for a corporation running multiple medical centre operations, one would have to question the impact of a short spell of bad press.

Furthermore, this says nothing of on-sold data that is 'de-identified'. Under the new Guidelines, "once data is de-identified, it no longer falls under the jurisdiction of the Commissioner" (Dearne & Spencer 2001: 26). Of course, this fails to consider the power of information technology to data match. As has been earlier noted, data matching (or computer matching) involves combining the information stored on two or more data systems, a type of reverse inferencing. In this way, multiple previously unidentifiable sets of information have the potential to become a single identifiable record, thus clearly referring to a unique identity.

Not only would on-selling de-identified information be legal, but it would also not require patient consent. Therefore, it is quite possible that under the new legislation a patient's sensitive 'de-identified' data is on-sold, without their knowledge or consent, only to be re-identified down the track.

Under the Guidelines, the Privacy Commissioner is clearly not adequately empowered to enforce patient information privacy and security. Perhaps a better method would have been in the implementation of privacy auditing. One expert referred to the success of the United Kingdom's privacy law. Through a body employed by the government, organisations are randomly audited to check for proper compliance with legislation, "reports by privacy auditors can assure individuals that organisations adhere to privacy standards and that those organisations that pledge to protect privacy actually do so." (Duff et al. 2001: 14).

Sweden is an example of another country that may hold some ideas that could also be investigated. With a long standing Data Protection Act, introduced in 1973, and an associated Data Inspection Board, Sweden employs a type of licensing system for those wanting to maintain databases (Greisser et al. 1980).

In this way, the Privacy Commissioner would not have to rely solely on complaints, and would be seen as actively pursuing offenders under The Privacy Act. Privacy audits, database licensing together with more serious sentencing, would be a better alternative in the enforcement of privacy law.

Conclusions and recommendations: are the Guidelines adequate?

The Draft Health Privacy Guidelines come as a welcome development in Australian health care legislation. In particular, the Guidelines bring about an open access ideal, where one can access, correct and in some cases remove personal health information. The Guidelines represent a considerable cultural and generational change to what private sector health providers can now do in dealing with patient information. Representing a firmer regulatory stance, the Guidelines impart requirements on the health care sector, incorporating the acquisition of consent, and procedures regarding information collection, use, disclosure, handling, management and storage.

Overall, the stance proposed by the Guidelines represents a great step forward in recognising the importance of health information privacy. However, The Guidelines appear flawed in their capacity to withstand a growing corporatised health sector. With little enforcement capability, the Guidelines cannot effectively ensure that personally identifiable health information will not end up in corporate third party hands. If this indeed occurs, privacy breaches will continue unpunished, thus ensuing in a loss of public faith. The result might be a growing number of people withholding sensitive information from their practitioners. While this might prevent them from possible discrimination, it can only be potentially harmful to their health.

An alternative or supplement to the Guidelines lies in explicit health data legislation, licensing and privacy auditing. In this way, the limited scope of 'consent' would be rectified by explicitly specifying who is entitled to access what information. Furthermore, privacy auditing would enhance information privacy by keeping organisations in compliance, thus promoting consumer confidence.

Society's (un)awareness about privacy rights has already been noted. So too has the corresponding value society places on privacy. It would therefore come as no surprise that commentators predict privacy will become good business (see Orr 1999: 68; Sprehe 1999: 19; Vincent 1999: 16). In this way, organisations would expose themselves to privacy auditors, thus building consumer confidence.

The amendments to The Privacy Act (1988) facilitate such a privacy conscious action. As part of the complement of guidelines extending the Act's scope, the 'Code Development Guidelines' are for any organisation seeking to develop a privacy code for subsequent approval by the Privacy Commissioner (OFPC (C) 2001: ix). Approval by the Commissioner in this area would help differentiate an organisation in their respective industry, thus increasing their commercial viability. It is aspired that health care corporations will take advantage of this provision, using it both to the privacy benefit of patients, and the commercial gain of their own organisation.

Summary of expert discussions

The primary aim of this research was to make an assessment of the privacy and security of personally identifiable patient information, as offered by the Draft Health Privacy Guidelines. Central to achieving this goal was the interviewing of key experts. All experts agreed to a rising air of public suspicion. This refers to society's general lack of confidence in the private and public sector and the secure management of their personal information.

While Australians generally trust health care organisations above others, concern still exists even at a local general practice level, independent of any other medical institution. Fuelling concern over a growing surveillance and control society is the corporatisation of health care. In this emergent environment, commercial style operations have the potential to create in-depth profiles of an individual's health. The on-selling of this information to insurers, banks, etc., could then see it matched with other personal information, making for an alarmingly detailed personal risk assessment, who would insure you and for how much?

There are deficiencies in consent requirements, together with feeble enforcement capabilities. This means that The Guidelines cannot effectively ensure that personally identifiable health information will not end up in third party corporate or government hands. In addition, requirements regarding health information collection generate further concern. In attempts to avoid obtaining consent in the future, practitioners may request secondary information under the fallacy of being within the scope of the health service sought. Given the power of information surveillance technologies, this disclosure of superfluous sensitive health information could adversely affect patients in the impending future.

To significantly bolster the Guidelines, it is suggested that they be supplemented with explicit health data legislation and privacy auditing. In this way, the limited notion of 'consent' would be rectified by explicitly specifying who is entitled to access what information. Furthermore, privacy auditing would enhance information privacy by keeping organisations in compliance, thus promoting consumer confidence. While the modifications to The Privacy Act (1988) facilitate the optional approval of privacy codes, it is aspired that this practice, along with privacy auditing, will eventually be universal. In this way, the market would be responding to society's increased awareness of privacy matters.

Recommendations for future research

The implementation of the Draft Health Privacy Guidelines/legislation represents a significant change to the current practices of private sector health providers. The topic will therefore remain relevant, especially until it is first reviewed in two years time. Prior to this review, a variety of impact studies could be undertaken on various aspects of health care. Firstly, this study alludes to the fact private sector health organisations will have difficulties complying with the new legislation. It would therefore be of interest to gauge this level of (non)compliance. The cost of compliance and the subsequent changes to common practice could all be highlighted. Conclusions drawn could point to how better to implement such influential legislation.

This study has also alluded to the Australian public's general level of privacy unawareness, in terms of both surveillance power, but especially privacy legislation. Also prior to the Guidelines' initial review, it would be of interest to assess the government's effectiveness in communicating its privacy regime. Of particular interest would be the public's level of awareness and knowledge of their specific privacy rights, as stemming from the Guidelines. Do patients know what their rights are?

It has been mentioned that this study's scope did not encompass judging whether The Guidelines would adversely affect the provision of care. Another possible project in its own right, an assessment could be made as to whether the Guidelines' limited view of consent actually makes for a greater or lesser quality of patient care. The notion of consent would also need to be reviewed in a growing electronic and biometric environment. How will patient consent be measured in the future?

Acknowledgements

We would like to thank the group of expert participants who were most obliging in offering their time and knowledge. Their invaluable contributions are sincerely appreciated.

References

Australian Medical Association (AMA) 2001, *The AMA's Submissions on Draft Health Privacy Guidelines.* URL: http://www.privacy.gov.au/publications/healthsubs/ama_sub.doc

Berg S & Davis M 2001, *New Health Privacy Guidelines*, Ward & Partners.
URL: http://www.wardpartners.com.au/Bulletins/Privacy_Guidelines_June_2001.htm

Bomba D & de Silva A 2001, *An Australian Case Study of Patient Attitudes Towards the Use of Computerised Medical Records and Unique Identifiers*, World Medical Informatics Conference 2001, London.

Brown P 2001, 'Privacy laws a Big Brother for most', *The Australian*, 17 May, p 21.

Carter M 1998, 'Should patients have access to their medical records?', *Consumers & Healthcare*, vol 199, no 11-12, pp 596-597.

Carter M 2000, 'Integrated electronic health records and patient privacy: possible benefits but real dangers', *Medical Journal of Australia*, no 172, pp 28-30.

Conlan M 2001, 'New medical privacy rules coming, with caveats likely', *Drug Topics*, vol 145, no 9, p 63.

Dearne K & Spencer M 2001, 'Privacy watchdog attacked', *The Australian*, 15 May, p 26.

Duff W, Smieliauskas W & Yoos H 2001, 'Protecting privacy', *Information Management Journal*, vol 35, no 2, pp 14-30.

Greisser G, Bakker A, Danielsson J, Hirel J, Kenny D, Schnieder W, Wassermann A, (Eds.) 1980, *Data Protection in Health Information Systems, Considerations and Guidelines*, North-Holland, Amsterdam.

Graves D 2001, *Consultation on the Draft Health Privacy Guidelines*, Royal College of Pathologists of Australasia
URL: http://www.privacy.gov.au/publications/healthsubs/rcpa_sub.doc

Hoffmann M 2001, 'Problems with privacy', *Business Insurance*, vol 35, no 17, p 6.

Kay H 2001, *Submissions on the Draft Health Privacy Guidelines*, Law Reform Commission of Western Australia, Perth.

Lyon D 2001, *Surveillance Society*, Open University Press, Buckingham.

McMenamin B 2001, 'Prescription For Snooping', *Forbes*, 28 May 2001, p 62.

Mitchell R 2001, 'Risk managers apprehensive over new medical privacy rules', *National Underwriter*, vol 105, no 19, pp 68-69.

Mudge T 2001, 'Unhealthy access to medical records', *Newcastle Herald*, 17 May.

Office of the Federal Privacy Commissioner (OFPC) (A) 2001, *Draft Health Privacy Guidelines.*
URL: http://www.privacy.gov.au/publications/dhgd.html

Office of the Federal Privacy Commissioner (OFPC) (B) 2001, *Privacy and the Community.*
URL: http://www.privacy.gov.au/publications/rcommunity.pdf

Office of the Federal Privacy Commissioner (OFPC) (C) 2001, *Guidelines on Privacy in the Private Health Sector.*
URL: http://www.privacy.gov.au/publications/nppgl_01.pdf

Orr B 1999, 'NCR to banks: Privacy is good for business', *American Bankers Association (ABA) Banking Journal*, New York vol 91, no 6, p 68.

Sprehe T 1999, 'Privacy policies should not be optional', *Federal Computer Week*, Falls Church, vol 13, no 13, p 19.

Stock S 2001, 'Privacy push opens files to patients', *The Australian*, 14 May, p 3.

Vincent L 1999, 'Profiting from privacy', *Bank Marketing*, Washington, vol 31, no 9, pp 16-17.