SecureNet

SecureNet Limited
Level 3, Saunders St
Pyrmont NSW 2009

National Health Privacy Working Group Secretariat
MDP 66
PO Box 9848
Canberra ACT 2601

18 April 2003

Dear Sir/Madam

Submission on the Discussion Paper "National Health Privacy Code (Draft)"

We are happy to make this submission on the Draft National Health Privacy Code, and to participate in the ongoing deliberations over electronic health records and e-health in general. SecureNet commends the Working Group on the Draft Code.

SecureNet is a successful Australian specialist provider of information security services and products. We have particular interests and experience in e-health and privacy, and hence we are keen to contribute to important peak strategy and policy work in the area. We have contributed much in recent years to public consultations and strategic reviews, on topics including a range of privacy related projects, the NHIMAC review and the National Authentication Technology Framework development. Some relevant corporate background on SecureNet is provided in an Annex to this submission.

General Comments on Health Privacy

Catering for covert collection of Health Information

It strikes us at SecureNet that when most people think about the collection of personal information, by default they generally imagine direct collection methods, like forms and face-to-face interviews. Yet electronic information handling leads to other indirect types of collection. As far as we can tell, privacy legislation does not differentiate between methods of collection; all personal information is to be safeguarded regardless of how it is gathered.

Personal information can be collected in at least five different ways, and we believe it is important to anticipate and plan for different privacy problems under each category. SecureNet defines the categories as follows:

1. ***Overt (or Direct) collection*** via application forms, web forms, questionnaires, face-to-face interviews, call centre interactions, returned warranty cards etc.

2. ***Automatic collection*** especially via audit logs and transaction histories.

3. ***Information generation*** includes opinions, evaluative data and inferences drawn from collected personal information, for the purposes of service customisation (such as direct marketing programmes fine tuned in response to established buying preferences), business risk management (such as calculating insurance premiums or no-claims bonuses according to risk scores calculated from claims histories) and so on.

4. ***Acquired information*** is that which has been transferred from a third party, with or without payment for the information, including cases where personal information is acquired as part of a corporate takeover.

5. ***Ephemeral information*** is a special category of automatically collected or generated data, produced as a side effect of other operations. Ephemeral information is reasonably presumed to be transient but can be inadvertently retained. For example, some operations prompt users for a pre-arranged secret – classically their mother's maiden name – when dealing with a forgotten password. The secret information can be left behind in computer memory or logs, or scribbled on note paper by a help desk operator. Other sources of ephemeral personal information include printer spooler memory, browser cache memory, and network servers where temporary copies of information-in-transit can be retained.

We note that the Draft Health Privacy Code deals expressly with overt collection, generated and acquired information, but does not seem to anticipate any type of automatically collected information.

The ubiquity and transparency of automatically collected information within e-business and e-health systems presents a host of serious challenges in respect of scope creep, information leakage, and the ability to locate and remove all of an individual's records.

We shall cover some specifics elsewhere in this submission, especially in relation to various questions of practicality.

The standing of doctors' notes

One area of historical contention has been whether or not a doctor's evaluative notes and opinions written into a patient's record should be treated in the same way as all other patient information. There has been a view that the doctor's notes are their intellectual property and ought not to be automatically made available to the patient.

SecureNet takes no position on this debate; we only note its importance on a number of fronts, including practical matters of access control, consent and custody. These information management aspects are strongly impacted by whether or not different parts of a record are deemed to have different owners.

We understand that matters of doctors' intellectual property and ownership of the patient record have been ruled upon in recent years in various courts and other fora. We suggest that for clarity the preamble to the Code contains a recap on these issues, to clarify the standing now of doctors' notes.

The employee records exemption of the Privacy Amendment (Private Sector) Act

Employee records are exempted by current private sector privacy legislation. Employee records can of course contain health information. Is there any intention therefore for the Health Privacy Code to undo the employee records exemption?

Responses to some of the specific questions

To help us develop and present some of our arguments, please note that we have answered some of the questions out of numerical order.

Q9. Do other types of information need to be added to the definition of 'health information'?

Yes. We believe that there is behavioural and attitudinal information that may be strongly predictive of a person's state of health (or of their belief as to their own state of health), which should therefore be added to the definition of health information. We suggest that the following types of information be included in the definition:

- diet and eating habits
- sports and exercise regime
- usage of non-prescription medications
- usage of herbal and non-traditional remedies.

We note that the current definition of health information includes "genetic information … which is or *could be* predictive (*at any time*) of the health of the individual …" (emphasis added). We suggest that the predictive power of information about diet and exercise is stronger today than is almost any genetic information at hand, and is therefore just as deserving (if not more so) of inclusion in the definition.

Q6. What would be the most reasonable and appropriate approach [to the scope of the Code] to take?

We strongly support Option 2, where the scope of the Code is broad enough to cover all organisations handling health information of any individual. Thanks to e-commerce, there is a fast growing array of non-health organisations capable of compiling rich veins of health-related information about individuals. For example:

- Bookstores and libraries tracking interest in self-help books can determine what their clients at least *believe* they suffer from, if not what their medical conditions actually are.

- Grocery stores with regular customers can determine in great detail the eating habits of families and individuals.

- While herbal remedies remain generally available from supermarkets and retail outlets, these organisations too can work out what some of their customers may

believe they suffer from. For example, regular purchase of St Johns wort is very likely to indicate a depressive illness, real or imagined.

- Department stores and sporting goods outlets can characterise the exercise habits and related state of health of their regular customers.

- Regular fast food deliveries will be significantly predictive of overweight and obesity, and associated medical conditions.

- Internet search engines can often identify the source IP address of each individual inquiry, and if collected can obviously represent a rich source of health information.

- Internet fridges are capable of fine-grain tracking of what and when people eat. It is not yet clear which types of organisations are going to be collecting this information as Internet fridges and other domestic appliances penetrate the market; if whitegoods manufacturers can collate the data automatically, then there could be a ready market for the information. There are clear health privacy implications.

If the definition of health information was to include diet and lifestyle information (as discussed under Question 9 above) then there is a strong case that any organisation handling such information – including bookstores, Internet search engines, grocery outlets and fast food companies – should be covered by the Code.

Q2: Are there specific aspects of the electronic record and the way it operates which indicate the need for additional standards?

Yes. Electronic information storage and handling is characteristically different from paper systems in ways that not only exacerbate threats to privacy, but which in many cases also impinge on the very practicality of privacy safeguards.

Compared with paper systems, electronic information and records:

- are far more easily aggregated
- are far more easily indexed
- can be searched quickly by brute force
- are content-addressable (leading to privacy threats like the reverse White Pages)
- can be collected automatically and covertly
- can be copied with negligible cost and delay, almost without limitation
- if they are the original instance of some information, generally bear no intrinsic signs or clues to mark them as original, as opposed to copies
- can be copied without being noticed by the owner
- are inadvertently (and almost unavoidably) copied as a side effect of being accessed, used or transmitted
- can be undetectably modified, at least locally[1]
- are much easier to destroy than paper, at least locally[2]

[1] That is, information stored within a local computer can be modified without any trace being left of the tampering. Copies of the original information might exist somewhere away from the local computer, and these might be pressed into the service of forensic investigations of what happened to the local copy.

- usually cannot have new types of information freely added to the record without significant re-design and upgrade; in particular, free-text annotations cannot usually be readily made against arbitrary fields in the same way as handwritten notes can be made anywhere on a paper record
- because they are stored by 'smart media', are subject to viruses.

There are many implications of these characteristics of electronic records, and the threats that arise to privacy are well documented. Rather than re-hash the threats, we would like to make a few observations about the practicality of translating certain privacy safeguards designed for paper systems into the electronic world.

1. The ubiquity of automatically generated personal information (captured in audit logs for instance) and of inadvertent copies (backups, copies on e-mail servers etc.) can make it difficult to be able to fully comply with requests to access and correct all information held on an individual. There may be technological solutions to help ease this problem, such as intelligent agents that seek out audit logs and copies of records. It is important in general that privacy policies and standards are informed not only by the idea of directly collected information, analogous to traditional paper based collection, but also by the reality of automatically collected electronic information.

2. Traditional databases are notoriously inflexible when it comes to attaching ad hoc annotations to particular records or fields within records. So where privacy standards require that annotations be made to a record concerning consent matters for example, or disputed updates, we need to understand that many existing data systems are likely to make this task very difficult.

3. Version control and automatic backup have not historically been well designed features of data systems (if they are featured at all). This poses difficulties for that requirement in the Code that old information in general never be deleted, even when found to be incorrect. It means that great care shall have to be taken to preserve the old records when correcting health information. In many systems it is likely that a manual backup of the old file shall have to be made and archived first. Procedures for making backups and labeling and storing them will be needed.

We shall return to these practical issues in some of the other detailed questions below.

Q39: Should the aim of NHPP 5.2 be to provide information when requested to a specific individual … or should it aim to make general information available to anyone?

It would be outside the scope of a Health Privacy Code to try to anticipate and cater for making general information available to anyone. NHPP 5.2 should only concern itself with providing health information to specific individuals.

---

[2] To totally destroy paper records usually requires a major catastrophe, like a severe fire. The local copy of electronic records however, can be laid to waste utterly in any number of ways, including the failure of a trivial computer component, a power supply glitch, user error, or a virus.

Q42: Are the … exemptions to providing an individual with access to his/her health information reasonable?

It appears to us that the exemption at 6.1(d) has been lifted without much change from the NPPs and may be misapplied in the field of health information. We cannot imagine a case where a health organisation is negotiating with a person on matters outside the context of their personal health, but where that person's health information is somehow pertinent to the negotiation, to the possible advantage of the organisation. And even if such a case were to arise, what legal principle weighs in favour of the business interests of the organisation over the privacy interests of the individual?

Q47: Do [the provisions relating to correction] adequately cater for correction of records regardless of format … ?

No, not really. As discussed in general terms above in Question 2, the difficulty of making annotations outside the design parameters of an existing database, and the generally poor state of version control functions and procedures, means that some privacy standards might not easily translate from the paper format to the electronic. In particular:

- NHPP 6.5 states that when correcting information, the organisation "must not delete information unless authorised to do so under NHPP 4". If the data system does not support rigorous version control and automatic backups, then it may be necessary for manual backups to be made to preserve the old information.

- NHPP 6.7(b) anticipates situations where "the form in which the health information is held makes correction impossible". In the case of electronic information systems, "impossible" can be a very tough test. Most if not all software is modifiable given sufficient means, by upgrade or re-write as applicable. There will be few if any situations where correcting an electronic record is truly impossible. We therefore suggest changing "impossible" to "impracticable" at NHPP 6.7(b).

- NHPP 6.8(a) requires the name of the person making a correction, plus the date of the correction, to be recorded with the correction if practicable. If the data system has not been expressly designed or configured to record this type of information, then it is unlikely to be practicable. We think it would be unfortunate to adopt a Code if a particular clause like 6.8(a) was found to not apply in a great many cases.

Q55: Are there any issues regarding the use of unique identifiers … ?

NHPP 7 as drafted appears to take an almost opposite stand on the re-use of government issued identifiers compared with the National Privacy Principle 7. NHPP 7 broadly allows for government issued identifiers to be re-used by health sector organisations, whereas the National Privacy Principle 7 basically forbids it.

The Consultation Paper on p38 says that "[NHPP 7] recognises that there are other laws relating to the use of identifiers" but provides no further detail on how this 'recognition' is manifest. As the Code stands, it is not clear how we should reconcile NHPP 7 and NPP 7.

Q79: Should the law prevent or regulate the selling of [non-identifiable] data?

We recommend that great caution be applied to the handling of purportedly non-identifiable or de-identified data. De-identification is always a statistically based operation; no meaningful data can ever be safely regarded as absolutely non-identifiable.[3]

De-identification can be infeasible in cases where only a few individuals in a sample exhibit a rare medical condition. Yet inclusion of records from such individuals can be highly desirable for research purposes. For instance, if just one or two people in a country town have some drug addiction, that fact may be important for public health planning. But de-identifying information about drug addicts can be difficult in a small population, especially if they are young and exhibit other unusual traits.

The effectiveness of de-identification needs to be carefully determined according to the type of information concerned and the statistical characteristics of the population from which it is collected. The context of the researcher is important too. For example, de-identified data from a particular Eastern Australian locality might be non-identifiable for a researcher based in Perth, but if it was to become available to someone who lived in the town from where it was sampled, that person might be able to discern patterns and work out identities.

The potential ability to re-identify individuals in a de-identified data set depends on technological advances and can be facilitated by the future aggregation of other intersecting data on the same individuals. If we cannot confidently rule out future advances or the aggregation of further data, then we should probably treat all de-identified data as potentially re-identifiable. There should be strict controls over the distribution of de-identified data. And there is a need for statistically robust de-identification standards and hands-on guidelines to be made more widely accessible.

Miscellaneous comments on the NHPPs

- NHPP 1.4(f): We suggest changing "if all or part of the information is not provided" to "if all or part of the information is not collected" since it is not necessarily the case that health information needs to be directly provided by the individual.

- NHPP 1.7(i): We suggest changing "confirm with the person" to "confirm with the individual" since the term "individual" is used throughout the rest of the clause.

- NHPP 6.6(a) seems uncharacteristically weighted towards the rights of health organisations, by allowing for an organisation to be simply "not willing to incorporate the correct health information". There is no such latitude granted to organisations in the corresponding clause of National Privacy Principle 6. Why should the standard be so different when it comes to health information?

- NHPP 7.2 refers in two places to "State or Territory public sector organisation". Is it deliberate to exclude the Commonwealth public sector from these clauses?

[3] In the second paragraph of p50, the Consultation Paper says of non-identifiable data that "an individual's identity is not apparent and *cannot* be reasonably ascertained in any situation." (emphasis in original). We suggest that this is too tough a test.

- NHPP 11.1(iii) refers to a "summary of the individual's record". Are there any standards or guidelines in place yet for the creation of "summaries"?

Conclusion

We expect that the focus of the Working Group to this point has been to develop a set of minimum standards with general and widespread applicability. Doubtless, the Working Group already anticipates as a next step the preparation of detailed guidelines to inform the implementation of e-health systems and the day-to-day activities of healthcare workers, to minimise breaches of the NHPPs. Such guidelines would parallel the recently released guidelines of the RACGP for the security of medical records.

It seems clear to us that detailed guidelines should be developed to cover issues including:

- de-identification of health information
- effective means for locating all records stored across diverse and heterogeneous information systems relating a given individual
- processes for the reliable retention of old information where information handling systems do not feature robust version control or automatic backups
- satisfactory means for properly deleting stored electronic data when required.

Thanks again for this opportunity to engage in this most important national consultation. We hope our comments are of some value. SecureNet would be happy to participate in any follow-up dialogue or discussion forum, particularly focusing on the next steps of developing implementation guidelines. And we look forward to seeing further progress from the National Health Privacy Working Group.

Sincerely,

Stephen Wilson
Principal Consultant

Annex: Background on SecureNet Limited

Overview

SecureNet is a leading provider in Australia and Asia of e-business transaction security solutions. The business is broad-based, ranging from smartcard technology, public key infrastructure (PKI) and security components to secure payments, electronic transactions, secure gateway provision, managed security infrastructure and security consultancy.

SecureNet's operations began in 1982 and the company was listed on the Australian Stock Exchange in 1997 (ASX:SNX). Since then the organisation has expanded in both domestic and international markets, forming joint ventures and strategic alliances with leading IT&T organisations in Hong Kong, greater China and other Asia Pacific regions.

SecureNet is headquartered in Sydney, and has offices and facilities in Canberra, Melbourne, Hong Kong and the Peoples Republic of China.

The company operates three lines of business: *Professional Services* (comprising independent consulting in strategy and policy, security reviews, and security systems integration), *Trust Services* (including managed security services, perimeter security outsourcing, and PKI) and *Products* (including smartcards, secure e-mail and security servers).

Selected e-health and related experience

SecureNet has undertaken several significant projects in the health sector in recent years, leveraging our expertise in authentication, smartcards and government electronic services delivery. We are also active in allied government policy areas concerning authentication, PKI and smartcard applications. Of particular note are the following:

- Provider of PKI services to the HIC's Health eSignature Authority
- Conducted an IT Strategy review for the Victorian Department of Human Services' I2T2 Strategy development
- Principal Consultants on smartcard policy, privacy framework and security architecture for Hong Kong Immigration Department's new national ID card
- Corporate member of CHIK Services
- Developed data structures and business logic for Standards Australia's IT/14/10 Health Supply Chain Reform project
- Developed and implemented patient & provider smartcard systems for the Dandenong HealthKey trial for Victorian DHS, Commonwealth DHAC and Southern HealthCare Network
- Implemented smartcard systems for concession card holder discount scheme for Victorian Taxi Directorate
- Wrote the all-of-government smartcard strategy for Multimedia Victoria.