Australian Privacy Foundation

post: GPO Box 1196
Sydney NSW 2001
phone: +61 2 9231 4949
facsimile: +61 2 9262 3553
email: mail@privacy.org.au
web: www.privacy.org.au

Submission on the Draft *National Health Privacy Code*

issued by the National Health Privacy Working Group of the Australian Health MinistersÕ Advisory Council

April 2003

Contents

Introduction

The Australian Privacy Foundation (www.privacy.org.au) welcomes initiatives to ensure that the privacy of health information in Australia is protected in all circumstances. We commend the Working Group for raising awareness about the need to improve current safeguards.

Health information must be protected to nationally consistent standards that are strong, enforceable and easy to understand. This is common ground. The problem is working out how to achieve it.

Unfortunately, the Draft Code is not the solution. The protection it proposes modifies the national standard set out in the National Privacy Principles (NPPs) in the *Privacy Act 1998* (Cth), but it neither strengthens the NPPs nor broadens their scope.

Even though the code overlays the operation of an assortment of laws and administrative rules, the Working Group has stopped short of recommending how it should be transformed from good intentions to legal obligations.

The code is at risk of simply adding to the ever growing collection of voluntary and mandatory privacy principles in Australia, creating confusion and obfuscation without appreciable improvement to privacy protection.

Publication of the Draft is nonetheless a valuable opportunity to find ways to improve the protection of health information, and this submission is intended to contribute constructively to that end. We do not individually address each of the 82 questions posed in the consultation paper, although our comments touch on many of the matters they raise. Instead, we focus on how well the Draft Code achieves its own aims.

1. Safeguarding the health, privacy and dignity of all individuals

The first stated aim of the code is to safeguard the health, privacy and dignity of all individuals. This means establishing a strong and enforceable standard that those who apply the principles, and those who benefit from them, can understand.

The consultation paper does not explain why the Working Group believes the current national standard of privacy protection is inadequate, the weaknesses it is trying to redress, and in what way the standard it proposes is better. The apparent intention is to effectively replace the Commonwealth NPPs, as the national standard for health information privacy, with the Health Privacy Principles (HPPs) in the Victorian *Health Records Act 2001* (Vic).

The Victorian HPPs are similar to the Commonwealth NPPs but with some modifications. They set out more detailed rules for providing people with access to their own information in the private sector and facilitate the flow of information between public and private health service providers and government agencies.

As the *Health Records Act* covers the handling of health information by any organisation, regardless of size, it applies to small businesses that do not have to comply with the NPPs.

Although in some respects the Victorian modifications to the NPPs strengthen the standard of protection, in other respects they weaken it. Simply adopting the Victorian modifications is not a necessary or sufficient solution to ensuring that health information is adequately protected in all circumstances.

1.1 Scope of national health privacy regime

As health information must be protected to a higher standard nationally, we support measures to ensure that it is protected by any organisation that holds it.

The Australian Privacy Foundation has consistently opposed the extensive exemptions from the *Privacy Act* for private sector organisations. Any initiative to improve health information privacy must encompass all of the private sector.

The public sector in every State and Territory should also comply with legislation that guarantees at least this standard of protection.

1.2 Scope of the draft National Health Privacy Principles

Both the Commonwealth NPPs and the Victorian HPPs fail to address adequately some of the most pressing risks to health privacy. This weakness is now reflected in the Draft Code.

For example, the NHPPs in the Code should deal squarely with the following issues.

- **Definitions of ÔprimaryÕ and ÔsecondaryÕ purposes**. These terms can and should be defined more precisely in this context.

  Reference to a ÔprimaryÕ purpose could be defined as the collection and use of health information *in providing a health service to the person concerned*. The ÔsecondaryÕ purpose would then be defined as any other purpose.

  Collection, use and disclosure of health information in providing a health service to the person concerned could be subject to rules that are appropriate to health service providers. Handling of health information for all other purposes would be subject to rules that directly address the risk of misuse and unauthorised disclosure in these cases.

- **Management of health information databases and the accountability of those who manage them**. Some collect a great deal of sensitive health data with little or no authority under law and perhaps without the personÕs knowledge and consent.

- **Collection of health information from current or prospective employees** This includes assessments that purport to indicate psychological attributes and emotional stability. Such activities can have a crucial bearing on an individualÕs employment and promotion prospects.

- **Collection and processing of genetic data for purposes other than to provide a health service to the person concerned**. The sensitivity of this information calls for

additional protections yet currently it may be collected, used or disclosed with no more than implied consent.

- **Collection of health information for research**. This is apparently left to guidelines yet to be specified or written. There is a clear public interest in conducting research. There are also well-founded concerns in about the consistency of the application of ethical principles in relation to research using sensitive information, both at the time of the research and in later years. How medical research can be conducted so that the public interest in protecting privacy is also preserved should be transparent. The viability of some types of future research may depend on public confidence in privacy protection, and this confidence will be eroded if this increasingly significant issue is not dealt with in the Code.

1.3 The level of protection required

The Commonwealth NPPs do not currently provide an adequate national standard of protection for personal information. Producing a draft National Health Privacy Code provides a valuable opportunity to revisit and improve them.

Unlike the NPPs and other provisions in the *Privacy Act*, the Draft Code establishes detailed processes for providing the individual concerned with access to their health information. These processes would apply only to the private sector, as access to public sector information is regulated by Freedom of Information legislation or other laws. They set out processes that organisations can follow in responding to requests for access, improving the individualõs right to receive at least some information when unfettered access is denied.

Nonetheless, it is not clear why the Draft Code goes to such detail in setting out the access provisions.

If this level of detail is required, would it be better forming part of an attached Schedule of procedural guidelines?

Why not also provide a similar level of detail about other circumstances where the organisation holding the information has to exercise judgment? For instance, when releasing information to law enforcement agencies, or when deciding whether to rely on express consent or implied consent, or how to respond to a complaint about a breach of the principles?

Compared to the Commonwealth NPPs, the NHPPs in the Draft Code add to and clarify the purposes for which health service providers and government agencies may collect and use health information without the personõs knowledge or consent.

These purposes are in the personõs interest or the public interest and in general we do not object to them being accommodated in a national standard, though in some cases privacy has been eclipsed to an unacceptable degree.

For organisations other than health service providers, the proposed standard is either unchanged or possibly lower than presently required by the NPPs. This is of significant concern. Wherever health information may be collected and used for purposes other than providing a health service, the risk to privacy is high. To reduce the current standard is unacceptable and unjustified.

Some examples of improvements that should be made are set out below.

- NHPP 6.1(c) permits organisations to deny individuals access to health information about themselves because of *anticipated* legal proceedings (emphasis added). This sets the standard too low, because this excuse can readily be invoked in too many circumstances. Under this provision, information could be withheld on the basis of mere suspicion or conjecture, and could even become a matter of routine. It legitimises a pre-emptive approach dependent on the attitudes and fears of the record holder, rather than any objective external fact. Should legal proceedings eventuate, the rights of the parties are protected by laws of evidence and judicial processes. This exemption should be removed.

- While the NPPs recognise that personal information (including health information) may be collected, used and disclosed as "required" by law, the NHPPs allow this to occur where "required, authorised or permitted, whether expressly or impliedly" by or under law — NHPP1.1(b); NHPP2.2(c). If there is a public interest in collecting and processing health information without the person's knowledge and consent, the relevant government authorities should be expressly empowered to do so, and specifically held accountable for how they exercise that power. Allowing exceptions to the principles where "impliedly permitted" by law leaves little privacy protection at all. This exemption should revert to the more stringent NPP standard, where an express requirement is needed.

- The discretion to disclose for compassionate reasons should be removed or tightened — NHPP 2.4(b). It does not specify to whom the disclosure may be made and the term "compassionate reasons" is imprecise, and in these circumstances is too open to inappropriate personal interpretation.

- The NPPs allow for personal information to be collected without consent for research relevant to "public health or public safety". The NHPPs allow the collection of health information for research in the "public interest" generally. This is far too broad. Many activities, objectives and ideals may be described as being "in the public interest", yet not all should compromise the right to privacy. There is no satisfactory definition, test or stable accepted meaning of the term "in the public interest". This exemption should revert to the more stringent NPP standard.

- Individuals do not need to be told, even in general terms, who will see their health information when it is used or disclosed for training purposes by a health service provider, or for the funding, management, planning, monitoring, improvement or evaluation of health services by any organisation — NHPP1.6. This seriously reduces the accountability of those who handle health information for secondary purposes, where privacy is most at risk. At least a general and preferably a fairly specific description of such disclosures should be mandatory.

  In addition, the distinction between "monitoring, improvement or evaluation of health services" and medical research is in practice so fine as to be non-existent, and this provision is therefore likely to become a source of confusion or obfuscation.

- There is no requirement to make a written record of having used health information for law enforcement purposes — NHPP2.3. As there is a public interest in law enforcement, those conducting law enforcement activities should be accountable for how they do so,

especially where other interests and rights are infringed. A written record should be mandatory.

In addition, there are frequent examples of abuse of law enforcement systems by individuals with privileged access for personal or other improper reasons, and only a written record requirement can assist in auditing any such activity.

- The definition of which agencies' law enforcement functions need to be accommodated should also be reviewed. The current definition of 'law enforcement agency' includes the Australian Prudential Regulation Authority, the Australian Securities and Investments Commission and other government agencies whose law enforcement activities are unlikely to require them to collect health information. Should it be necessary in exceptional circumstances, those agencies should rely on their own legislation for the necessary legal authority.

- Any organisation can refuse to disclose to the person concerned any health information it has collected from a third party (other than an authorised representative or a health service provider) if the third party so requests — NHPP6.1(e). This is an extraordinary provision which reverses the usual obligations to the data subject, and could act to prevent appropriate accountability of such disclosures. It is the antithesis of fair information privacy practices, and must be removed. If the aim is to protect the third party from harm, this is already provided by NHPP6.1(a).

The *Privacy Act* is due to be reviewed at the end of 2003. It is recommended that the Working Group revise the NHPPs with a view to improving the current standard of protection, and submit them for consideration by the federal Privacy Commissioner in assessing the effectiveness of the NPPs.

2. National consistency

The second aim of the Draft Code is to 'achieve national consistency in health privacy protection - across jurisdictions and between the public and private sectors'

National consistency should not be seen as an end in itself, but as a means of developing a strong and enforceable privacy regime. It is most important to be clear about what needs to be consistent, and why.

2.1 Health v. non-health organisations

While there are sound arguments for requiring health service providers to protect the privacy of health information to the same standard throughout Australia, it does not follow that all non-health service providers should therefore comply with a consistent standard as well.

It may be quite reasonable to impose stricter rules and tougher penalties where the information handled is particularly sensitive, or the consequences of misuse harsher.

Health information collected and used by welfare agencies, for example, or insurance firms, employers, and others whose decisions can fundamentally affect the lives of the people concerned, may need stronger safeguards. They could be required to get express rather than implied consent, or refrain from activities that are seen as coercive or unduly intrusive.

We submit that consideration be given to requiring certain (typically non-health service provider) organisations to comply with such stricter protections.

2.2 Different laws override the Code

Even where national consistency could improve the standard of privacy protection, the Draft Code does not deliver it. All existing legislation that affects the handling of health information would take precedence over the national standard. In effect, there will be very little consistency from one jurisdiction to the next regarding how health information is handled in the public sector. Different laws will apply to the personõs right to gain access to their own health information and to the powers of government agencies to collect, use and share health information without consent.
Different regulations and guidelines may apply to the use and disclosure of health information for research, or in emergencies. Different laws govern the archiving and disposal of public records.

As information moves from one jurisdiction to the next, privacy safeguards will still be likely to change.

2.3 Variable application and enforcement of a voluntary Code

Another consideration is how consistently the standard will be applied and enforced. If it is only a voluntary standard of protection, there will be little consistency. It should be mandatory and legislated.

To achieve national consistency, each jurisdiction will need an independent compliance and complaint-handling authority with sufficient resources to perform the role. The NHPPs contain broad requirements to act reasonably, and this could be interpreted differently from one organisation to the next, and from one jurisdiction to another. The privacy watchdogs will need to work cooperatively to provide certainty for organisations and individuals alike, and be funded to do so. This must extend to delivering training and community education programs, as well as complaint handling, auditing, and advisory services.

Consistency of health privacy protection is therefore not only a matter of agreeing to a set of NHPPs. It requires a commitment by all governments to legislate for and enforce a national approach.

2.4 Uniform national legislative framework is needed

It is recommended that the Working Group recast the code, with strengthened and expanded NHPPs, as

- draft legislation to amend the *Privacy Act* for the handling of health information in both the Commonwealth public sector and the private sector nationally, and
- draft model health privacy legislation for the State and Territory public sectors to adopt the same standard of privacy protection nationally and establish the necessary compliance and complaint-handling authorities.

3. Technological change

The final aim of the Draft Code is to ÔtakeÕ into account changes in the way personal health information is handled as a result of technological changeÕ.

3.1 Technology-neutral principles, program-specific rules

It is appropriate that the NHPPs are technology-neutral, and that they guide the development of specific rules where necessary.

The necessity for additional rules arises not necessarily from the technology itself, but from the privacy implications of how it is applied to the processing of information in a particular health or research program. Initiatives such as Health*Connect* create risks that must be addressed by more than the general exhortations in the NHPPs to act reasonably.

The safeguards should be tailored to the program, and stronger sanctions applied to any breaches.

3.2 Technological change undermines assumptions over time

In general, the price of technological functions fall over time (see ÔMooreÕs LawÕ). The result is that intrusive practices which were once not economically or practically viable can become more feasible and attractive over time, as the cost of the necessary information processing transactions fall. This means that, notwithstanding some incremental improvements in privacy-positive areas such as data security, it is likely that technological change will increase risks to privacy by facilitating broader use, re-use and distribution. In turn, this will require more intense scrutiny over time to ensure the continued protective effectiveness of rules made for specific health programs.

Approaches such as monitoring, regular reviews, and ÔsunsetÕ clauses can be used to facilitate revisiting the continued relevance of the assumptions underpinning such technology-specific program rules. Assumptions which were reasonable when a specific programÕs health privacy protection rules were initially developed (often before the commencement of the program) may cease to be reasonable if and when some unforeseen technological change or new application makes privacy intrusion significantly more practical or likely. The above approaches should be routinely used to identify and introduce any changes to program privacy rules that become necessary to maintain the original degree of protection in changed technological circumstances.

An associated safeguard is to require privacy impact assessments before new health and research programs and systems are implemented. Proposals would need to meet benchmark tests before moving forward. Privacy impact assessments should occur particularly when new technology is being proposed for implementation; but they are also indicated when applying older technology in a new way.

3.3 Specific examples of biomedical technology

Genetic, biomedical and biometric information and technology form a cross-over area with other potentially privacy intrusive developments. Further attention should be directed to current research and analysis of specific examples, such as the outcome of the ALRC Discussion Paper 66, *Protection of Human Genetic Information* (August 2002).

3.4 Further research on directions of technological development

Further research, publication and consultation are needed to ensure that there is sufficient public and expert appreciation of the range of possible future technological impacts on health care practice, research and health information privacy, as it is not clear the implications have been adequately taken into account so far. Organisations like the Centre for Health Informatics could assist in this technical research.

This work is needed to help assess whether the proposed NHPPs are sufficiently adaptable, general and truly technology-neutral to remain applicable in the face of unexpected future developments in technological capacity, applications, business practice, community norms and political trends.

Conclusion

The consultation paper and Draft Code have provided a valuable opportunity to raise the standard of health information privacy protection in Australia.

To meet the expectations of the Australian public for gradual improvement rather than incremental erosion of the protection of this increasingly critical information, the proposed National Health Privacy Principles need to be strengthened and broadened in scope and, most importantly, backed by legislation which gives them force and predictable application.