

31 May 2010

Graeme Osborne  
Chairman  
National Health IT Committee  
PO Box 5013  
**Wellington 6145**

Dear Mr Osborne

### **Comments on National Health IT Plan: Draft for Discussion**

I am pleased to be able to provide comments on this draft plan.

In general, I was happy to note the focus on person-centered health and the acknowledgement of the importance of consumer involvement in the implementation of the Plan. Some more specific comments, and recommendations, are attached.

As you will be aware I have a keen interest in the difficult but important task of developing a national electronic health information system that both supports the provision of care and protects the privacy of the people concerned.

Electronic health records give both health consumers and health agencies greater access to, and control over, health information. Accordingly they can present both privacy risks and benefits.

Privacy is a tool for protecting people's control of their own information, in the face of technological developments that might be used to lessen that control. Privacy risks need to be carefully considered when developing new health information systems, particularly given the increased focus on behavioural and lifestyle factors in person-centered health. Doing otherwise risks loss of trust and confidence from both clinicians and the public.

In my view, and with a mind to international experiences, there are clear risks from:

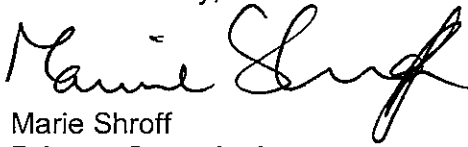
- electronic health records being collected and held without appropriate awareness or consent;
- the extension of national or regional health information collections into social indicators; and
- unanticipated secondary uses of collected data by researchers, social services and other public or private sector bodies.

If unaddressed, these risks may threaten both public confidence in the health sector and, ultimately, public health. This draft Plan provides an important opportunity to anticipate and address these risks on a national level.

P/0187 /A226344

We look forward to working closely with you and the health sector as the Plan develops.

Yours sincerely,

A handwritten signature in black ink, appearing to read "Marie Shroff". The signature is fluid and cursive, with a prominent loop at the end of the last name.

Marie Shroff  
**Privacy Commissioner**

## Specific Comments on draft National Health IT Plan

### “Person Centred Health”

Keeping people at the centre of decisions about how their health information is managed is crucial. Person-centred healthcare, a core purpose of the draft plan<sup>1</sup>, is intended to ensure a person's health information ‘follows’ him or her. This could make it easier for people to make decisions about their health information and to establish what is recorded about them, as well as improving the accuracy of clinical information by ensuring only “one source of truth”.

On the other hand, it is not uncommon for people to want to be able to protect their own information or parts of it, particularly around matters that are sensitive from a personal, family or cultural point of view. They may choose to do this either explicitly (by requesting that particular information not be shared) or by their choice of providers (going to different doctors for different aspects of their care).

Naturally there are considerations that compete with an individual's ability to have complete control over their own information, particularly clinical safety. Nonetheless if health consumers cannot control information held about them on a given system, it should be incumbent on the custodian of that information to be able to explain why.

Ultimately, good information practice is good business practice. The best way of achieving person-centred health that protects the privacy of the people concerned is to incorporate privacy into the design and implementation of new information systems – ‘privacy by design’ – by making it a consideration when assessing business cases for large scale investment.<sup>2</sup>

It would also be useful to consider the risks that each of the six focus areas may entail. This will help to give a full picture of the projected health information environment, both positive and negative.

For instance, one of the goals in the ‘Safe Sharing of Information’ focus area is for people to have direct access to their own health information by a computer interface accessible over the web. While this can be a very powerful tool for openness and information autonomy it also raises not inconsiderable security issues from viruses, malware, identity theft, computer loss, and snooping family members.

### *Specific Recommendations*

- Establish in consultation with the consumer forum, Office of the Privacy Commissioner and other stakeholders what level of control health consumers should expect to have over information held on national and regional collections of information.
- Include ‘privacy by design’ as one of the criteria for evaluation of business cases in section 10.3 of the draft Plan.<sup>3</sup> This would include both consideration of privacy issues by way of privacy impact assessment (as noted elsewhere in the

<sup>1</sup> Page 6, National Health IT Draft Plan 2010

<sup>2</sup> See <http://www.privacybydesign.ca/> for more details on the idea of ‘privacy by design’.

<sup>3</sup> Page 30, National Health IT Draft Plan 2010

draft Plan) and incorporating privacy protective measures such as direct patient access to their own information.

- Include risks as well as benefits in the six focus areas set out in section 6.2 of the draft Plan.

### “Ownership” of Health Information

*“Clarity of thinking around sharing patient information and involvement of consumers. The principle is that health information is owned by the individual person/patient with clinicians and health organisations having the role of custodians of that information. However this principle does not change the understanding that clinicians should share information to maintain continuity of care for patients (using their professional judgement).”<sup>4</sup>*

This is an encouraging statement of principle. We particularly support stressing the role of health agencies as trustworthy custodians of the health information they hold.

However we think it is important to note that health information is not *owned*. Instead, individuals have rights in respect of their own health information and health agencies have obligations in respect of that health information.

‘Ownership’ entails a particular bundle of rights and obligations. These rights include the right to destroy a thing that one owns, to change it at will and to prohibit anyone else’s access to it. These rights are generally not going to be applicable to consumers’ health information in such black and white terms.

While we absolutely do not wish to suggest a lower standard of care for health information than the one suggested in the paragraph quoted above, our concern is that any high level summary of the status of health information should be as accurate as possible, to prevent later confusion.

Another danger of ‘overpromising’ when it comes to health consumers’ control over their own information is that reasonable restrictions on that control (for instance where necessary for clinical safety) will seem less justified.

However if one of the proposals in the draft Plan is that health consumers should have all the rights associated with ownership in respect of their health information, this should be explicitly stated.

#### *Specific Recommendations*

- Explicitly note that the National Health IT Plan will give individuals a level of control over their own health information consistent with ownership of that information.
- Alternatively, rephrase the paragraph above – one suggestion for change might be:

*The individual person/patient has rights over their health information including the right to access and correct it. Clinicians and health organisations have the role of being trustworthy custodians of that information. Clinicians should*

<sup>4</sup> Page 7, National Health IT Draft Plan 2010

*only share information where necessary to maintain continuity of care for patients (using their professional judgement).*

### **Regional Clinical Data Repositories**

Regional clinical data repositories form the basis of national Shared Care, which is anticipated to be implemented in Phase 2 of the draft Plan.

This model is preferable to attempting a single, all-encompassing, electronic health record. Ultimately the goal is ensuring that all medical professionals have the information they need to provide treatment to their patients and we support this goal.

However large scale collections of health information carry both benefits and risks. Notably the potential for data loss or misuse on a vast scale is much higher. There is also a likelihood that third parties will be seeking bulk access or linking to data held on the repositories. As such, great care should be taken to ensure that regional repositories are secure, transparent and robustly governed, with regular audits to ensure that these qualities are maintained.

For instance, the Health Information Standards Organisation issued a Health Information Security Framework in 2009<sup>5</sup>. HISO recommends, in respect of this framework, that “a governance and management body oversee its implementation, that products and networks are accredited, and that there is on-going monitoring of security.” These recommendations may not be achievable yet, if the structures to implement them have not been created, but in our view they should be addressed as a high priority.

We also reiterate the suggestion above around incorporating ‘privacy by design’ into the development of regional repositories. Useful lessons, both positive and negative, may be learnt from the experiences of existing regional repositories such as Auckland’s Testsafe.

#### *Specific Recommendations*

- Ensure robust and transparent governance of regional clinical data repositories, including governing bodies that can make decisions on how and when information may be disclosed
- Make compliance with the HISO security framework compulsory, transparent and closely audited.
- Learn from experiences of existing regional repositories to avoid potential pitfalls

### **Health Information Sharing Outside the Health Sector**

Diet, exercise, purchasing decisions, domestic violence and smoking are all social indicators that have significant health implications. Given the sectoral focus on non-communicable diseases and lifestyle factors leading to ill health, it seems likely that the notion of what constitutes ‘health information’ will continue to expand.

The draft Plan refers, on page 25, to taking “opportunities to engage with other government agencies in the areas of Education, Social Development, Housing and Local Authorities”.

---

<sup>5</sup> <http://www.hisac.govt.nz/moh.nsf/indexcm/hisac2-standards-approved-hisf>

This is only a passing reference, but we are aware of strong pressures to share information much more widely in the government arena.

While we appreciate the drivers behind developing a wider conception of good health, particularly in light of the proposed 'Shared Care' model, there are significant risks that need to be addressed.

Most importantly, New Zealanders trust their health care providers implicitly.<sup>6</sup> This trust is something to be treasured, and sharing health information outside the sector carries a genuine risk of jeopardising it.

Also, there are strong ethical obligations of confidentiality around clinicians' interactions with their patients. If ignored, these constraints could lead to practitioners losing their own trust in the national system and patients being reluctant to share vital information, endangering the very goals the Plan seeks to achieve.

Naturally there will always be circumstances where information needs to be shared outside the boundaries of the health sector. However these should be carefully considered with a view to ensuring both compliance with privacy constraints and maximum transparency, both to patients and clinicians. Having clear privacy frameworks around regional and national collections clearly setting out the purpose for which the collections hold their information will assist.

#### *Specific Recommendations*

- Ensure that national and regional collections of health information have clear and robust privacy frameworks and governance arrangements
- Ensure, where information is to be shared with external agencies, that compliance and risks are addressed transparently such as by making privacy impact assessment reports and privacy policies publicly available

---

<sup>6</sup> 94% of people surveyed thought the health sector was 'trustworthy' or 'very trustworthy' UMR Survey 2009 <http://www.privacy.org.nz/media-release-new-umr-privacy-survey-results/>