Health Care and Policy Working Group

11th August 2020

Submission:

Revocation and replacement of the Health Information Privacy Code under Privacy Act 2020

1. Introduction

Thank you for this opportunity to comment on the draft consultation Health Information Privacy Code (HIPC). While it is proposed that the changes to the current HIPC are being limited to those necessary to align with the new Privacy Act including minor drafting modernisation, and that no substantive new policies are implemented, we make the following points:-

Given the nature, sensitivity and vulnerability associated with personal health information we believe the HIPC should include more detailed/specific protections /safeguards over and above those provided in the Privacy Act 2020.

These should include more specific requirements relating to

- informed and explicit consent for health information/data,
- anonymisation and de-identification of personal health information,
- appropriate use of NHI numbers,
- managing risks of re-identification, and
- requirements relating to images, video and other types of media on which personal health information may be processed.

If not included within the body of the HIPC then we recommend these requirements be included as a Schedule or Appendix to HIPC or as separate guidance. Refer to section 'Additional Recommendations' below.

This consultation coincides with the heightened interest in privacy of health information in the wake of recent privacy breaches that have received media attention.

The Privacy Act 2020 has clarified the definition of an agency and an agent relationship, including for overseas organisations. We note that the revised code does not refer to an agent relationship, except for potentially under 4(2)(j). In the current environment, many health agencies have agent relationships with multiple organisations who do not fall within the scope of the Health Information Privacy Code and therefore may not be aware of the additional requirements of the Health Information Privacy Rules. To mitigate this the revised code should include more specific reference to the application of the code to agents of health agencies.

We also note there are 16 references to “his or her” in the revised code. We recommend these are changed to “their” or similar to ensure that the code recognises gender diversity and is appropriately inclusive.

2. Comments on the draft Health Information Privacy Code

4 Application of code

Insert definition of ‘information’

There is no definition of ‘information’. A definition of ‘information’ should be inserted, clarifying that it explicitly includes information mediums: paper/hardcopy information, electronic data, images and photographs, audio, video, telehealth interactions, performance and audit data relating to medical and healthcare devices and services, health device and other mediums which may collect, process, store or transmit information relating to individuals’ health and disability support.

4(2)(j) and ‘agent relationship’

If it is determined that ‘agent relationship’ (per section 11 of the Privacy Act 2020) falls under 4(2)(j) then 4(2)(j) should be expanded to provide more explicit requirements and expectations on health agencies and the organisations they contract with. As written, 4(2)(j), listed within ‘Other’ applications does not adequately meet the requirements implied in the Privacy Act 2020.
If it is determined that ‘agent relationship’ belongs elsewhere in the code then the explicit requirements and expectations code should be inserted there.

Rule 1 Purpose of collection of health information

Subrule 1(2) pg 6

*If the lawful purpose for which health information about an individual is collected does not require the collection of an individual’s identifying information, the health agency ~~may~~ **shall** not require the individual’s identifying information.*

While the wording of subrule 1(2) is consistent with the Act ‘may’ is permissive and could allow identifying information to be collected when it is not required for the particular lawful purpose.
We also suggest Rule 1 is more explicit in requiring agencies to collect only anonymous health information unless de-identifiable or identifiable information is necessary to achieve the purpose of the personal health information; and that “anonymous” and “de-identified” are defined. The existing wording is passive by comparison.

Rule 2 Source of health information

Subrule (2)(c)(iii)

We don’t agree the new exception in the Privacy Act is adequately covered off by (2)(c)(iii). We believe the new exception (information privacy principle 2(2)(e)(v) “that non-compliance is necessary to prevent or lessen a serious threat to the life or health of the individual concerned, or any other individual” spells it out more and should be added as (h) (iv). Additionally, this should be limited by an obligation to collect, process or disclose only the information reasonably necessary to prevent or lessen such serious threats.

Subrule (2)(g) pg 7 and also Rule 10(1)(e) and Rule 11(2)(c)

We believe these subrules are open to broad interpretation and misinterpretation and should be the focus of more specific requirements relating to anonymisation and de-identification of personal health information, including management of re-identification risks. We expect these requirements to be applied consistently including when personal health information is used cross-sectorally e.g. Stats NZ IDI.

Retention of references to section 54 (now section 30 of the 2020 Act) in **rule 2, rule 10, rule 11**
We think they should be retained – may reduce the likelihood of this provision being overlooked.

Rule 3 Collection of health information from individual
Subrule (3) pg 8
While we support the intent in principle, we remain concerned that compliance with subrules (1) and (2) is often poor and/or inadequate and if that is not improved subrule (3) risks perpetuating people's lack of knowledge about what happens to their personal health information after it has been collected.

Rule 10 Limits on use of health information
Subrule 1(b) pg 12
Accept, but note this is open to broad interpretation.
Limitations on use should require agencies to process only the information necessary to provide a health or disability service, including sharing with third parties. Where possible, this information should be de-identified.

Subrule 1(e)
Refer to comments under Rule 2 subrule (2)(g)

Rule 11 Limits on disclosure of health information
Subrule (2)(c) pg 14
Refer to comments under Rule 2 subrule (2)(g)

Rule 12 Disclosure of health information outside New Zealand
As but one example, the increasing use of telemedicine is likely to result in increasing disclosure of health information outside New Zealand. Therefore Rule 12 is an important addition to the code.

Whether it provides adequate protection and safeguards for New Zealanders' personal health information is yet to be tested.

There should be proactive monitoring of compliance with Rule 12 along with some easy to understand explanations for health and disability service consumers as well as for health and disability service providers and their associated workforces and agencies.

Rule 13 Unique Identifiers
There is some concern the current structure with 13(2)(b) and 13(2)(c) has the potential to create confusion around whether NHI numbers could be used for statistical or research purposes. We suggest further clarification is required.

3. Additional recommendations

Anonymisation, de-identification, re-identification (particularly relevant but not limited to Rules 2, 10, 11)
We note increasing references to "de-identified" and "anonymised" information by agencies handling personal health information, the accuracy of these terms and the inferred safety of such information. For example, a media release on the 25 June 2020 by the Ministry of Health relating to COVID-19 stated *'[NHI] allows us to anonymise health information linked to patients and then allows patients or their tests or results to be traced and tracked by health services.'* Further clarification of

these terms and requirements for each is necessary to enable reasonable transparency, informed privacy notice and consent, and to properly assess privacy and re-identification risks.

Specifically, we recommend that anonymisation and de-identification are both defined as two separate classifications:

- Anonymised personal health information should include requirements for irreversible re-identification of personal health information, and not include any direct or indirect (quasi) identifiers. This should remain applicable as agencies acquire new personal information, but may be a time limited assessment (to recognise this may no longer apply as decryption technologies or image/video/audio recognition search engines become more advanced or re-identification via matching of reasonably public information).
- De-identified personal information should include requirements that prohibit the inclusion of direct identifiers and unique identifiers. Indirect (quasi) identifiers may be present but are not reasonably expected to identify individuals in combination, resulting in a variable re-identification risk. De-identified personal information could permit a risk based approach to privacy and personal health data management, including controls to prevent re-identification or matching of datasets.

It has been noted that some health ethics committees/boards require the collection of additional sensitive demographic information for health care and clinical research purposes in line with the MoH/Stats NZ ethnicity data standards. This presents a conflict with data minimisation/ purpose limitation requirements, and can significantly increase re-identification risk of otherwise anonymised data (more so these days than previously). There needs to be transparency around this risk if the conflict is not addressed.

We recommend additional organisational and technical safeguards are developed and included in, or as part of, the HIPC to protect against re-identification risk of de-identified and anonymised personal health information. These safeguards should apply to personal health information stored on the cloud or outside of NZ.

ENDS

Barbara Robson, Patricia Cunniffe, Paul Holmes, Natasha Mazey

Members, Health Care and Policy Working Group

Privacy Foundation New Zealand