Human Rights Commission
Te Kāhui Tika Tangata

Submission to the Privacy Commissioner on Amendments to the HIPC, TIPC and CRPC

Contact Person:

John Hancock
Senior Legal Adviser
New Zealand Human Rights Commission
johnh@hrc.co.nz

Submission of Human Rights Commission on Amendments to the HIPC, TIPC and CRPC

Introduction

1. The Human Rights Commission ('the Commission') welcomes the opportunity to provide the Privacy Commissioner with comments on the proposed amendments to the Health Information Privacy Code 1994 ('HIPC'), the Telecommunications Information Privacy Code 2003 ('TIPC') and the Credit Reporting Privacy Code 2004 ('CRPC').

2. The purpose of the amendments is to update each code to reflect the recent enactment of the Intelligence and Security Act 2017 ('ISA'). The amendments are primarily designed to authorise the disclosure of information to intelligence and security agencies ('IS agencies') under each code and, in the case of the CRPC, to enable IS agencies to carry out security clearance assessments.

3. While the amendments do not require disclosure, in practice health, telecommunications and credit reporting agencies will have to balance the right of affected individuals to privacy[1] against the converse right of the general public to safety and security[2] when considering disclosure requests from IS agencies. In order to ensure that they adminster this complex task in a way that maintains public trust and confidence[3], a transparent legal framework and a coherent, visible and effective oversight regime are essential[4].

4. The Commission considers that publicly available guidance notes should accordingly be developed to assist affected agencies when considering requests from IS agencies for personal information. In this case of the HIPC, an update to its extensive commentary will also be necessary. Given that these amendments engage the human rights obligations of both state and private sector organisations, the UN Guiding Principles on Business and Human Rights[5] will provide an important point of reference for the development of such guidance.

---

[1] International Covenant on Civil and Political Rights (ICCPR) Article 17

[2] Such as the right to life and the right to personal security (Article 3 of the Universal Declaration on Human Rights and Articles 6 and 9.1 of the ICCPR)

[3] See the commentary of David Anderson QC, *A Question of Trust, Report of the Investigatory Powers Review,* June 2015, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf, at p 245

[4] As See M Cullen, P Reddy, *Intelligence and Security in a Free Society: Report of the First Independent Review of Intelligence and Security in New Zealand*, 29 February 2016, paras 1.1-1.14 and 1.20-1.33 and Independent Surveillance Review, *A Democratic License to Operate, Report of the Independent Surveillance Review*, Royal United Services Institute for Defence and Security Studies, July 2015, https://www.rusi.org/downloads/assets/ISR-Report-press.pdf, paras 5.30-5.34

[5] http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

The HIPC

5. The amendment (HIPC Amendment No. 9) proposes to amend Rule 11(2) of the HIPC by inserting a new subrule (2)(da) as follows:

> *Compliance with subrule (1)(b)* [which requires authorisation of disclosure of health information by the individual concerned or the individual's representative] *is not necessary if the health agency believes on reasonable grounds that it is either not desirable or not practicable to obtain authorisation from the individual concerned and that:*
>
> – *(da) the disclosure of the information is necessary to enable an intelligence and security agency to perform any of its functions*

6. As with all Rule 11 requests, the decision to disclose rests with the agency subject to the code. This amendment expands the criteria to allow disclosure of information for enabling an IS agency to perform any of its functions. These functions are set out in sections 10-15 of the ISA and include:

    - Intelligence collection and analysis
    - Protective security services, advice and assistance
    - Information assurance and cybersecurity activities
    - Co-operation with the NZ police and NZ defence force to facilitate their functions
    - Co-operation with other entities to respond to an imminent threat

7. These functions are carried out in furtherance of the IS agencies principal objectives under the ISA[6] which are to contribute to:

    - The protection of New Zealand's national security
    - The international relations and well-being of New Zealand; and
    - The economic well-being of New Zealand

8. Conversely, Rule 11 of the HIPC has inherent implications for health and disability practitioners as to their duty to comply with and uphold the rights set out under the Code

[6] Section 9, Intelligence and Security Act 2017

of Health and Disability Services Consumers' Rights (HDC Code). The HDC Code provides, among other things, that every consumer of health and disability services:

- has the right to have his or her privacy respected (Right 1(2))
- has the right to have services provided in a manner that respects the dignity and independence of the individual (Right 3)
- has the right to have services provided that comply with legal, professional, ethical and other relevant standards (Rights 4(2))
- has the right to effective communication, including the right to an environment that enables open, honest and effective communication (Right 5)
- has the right to be fully informed, including any information required by legal, professional, ethical or other relevant standards (Right 6(e))
- has the right to informed consent, except where any enactment, common law rule or HRC Code provision provides otherwise (Right 7).

9. The commentary to the HIPC on Rule 11 provides health practitioners with useful guidance in exercising their discretion when considering a disclosure request. It emphasises that Rule 11 *allows* rather than *obliges* disclosure in the event an exception to the presumption of non-disclosure applies[7].

10. While proposed Rule 11(2)(da) does not appear to change this in any way, due to its nature a request from an IS agency for information is likely to generate an elevated response. In addition, the scope of the functions and objectives of the IS agencies are relatively obscure in terms of their relevance or application to the health sector and, as such, may not be well-understood by health agencies.

11. It will therefore be important to provide the health sector with additional guidance as to the implications of the proposed amendment, including guidance on the objectives and functions of the IS agencies. This ought to include an update to the current HIPC commentary on Rule 11. Health practitioners may also benefit from an additional guidance note to assist with their decision-making in the event that they receive a disclosure request from an IS agency. Given the implications that the proposed amendment may have for health practitioners in the performance of their duties under the HDC Code, the preparation of the guidance note may benefit from input by the Office of the Health and Disability Commissioner.

[7] https://privacy.org.nz/assets/Files/Codes-of-Practice-materials/HIPC-1994-incl.-amendments-revised-commentary-edit.pdf, p 61

Placement of the amendment

12. More specifically, the Commission supports the placement of the amendment under subclause (2) of Rule 11. This approach appropriately places the exception amongst the suite of exceptions to Rule 11(1)(b) set out under subclause (2), which includes "serious threat"[8] and "detection and investigation of offences"[9] exceptions.

13. Placement of the IS agency exception under subclause (1) brings it out of alignment with (and elevates it above) other similar HIPC exceptions[10]. It would also remove the requirement on the health agency under subclause (1)(b) to have first considered whether the individual concerned, or their representative, had authorised such disclosure. This requirement is unique to the HIPC and reflects the particular ethical duties that exist in the health sector. Removal of the requirement for health agencies to first consider whether authorisation would accordingly give rise to decisions that risk breaching health consumer rights under the HDC Code.

Recommendation 1:

a. **That the HIPC commentary is updated to include commentary on new Rule 11(2)(da) and its implications for health practitioners and agencies.**
b. **That a guidance note is developed in conjunction with the Health and Disability Commissioner for the purpose of assisting health practitioners in their decision-making under Rule 11(2)(da) when responding to a disclosure request by an IS agency.**
c. **That the proposed amendment is retained under subclause (2) of Rule 11.**

The TIPC

14. As noted in the information paper that accompanied the amendments, the proposed amendment is structurally aligned with the Privacy Act. The placement of the proposed amendment (new Rule 11(1)(ga)) fits logically into the sequence of exceptions, after the "serious threat" and "maintenance of the law" exceptions, and mirrors the amendment made to Information Privacy Principle 11 of the Privacy Act made by s 314 of the ISA.

[8] HIPC Rule 11(2)(d)
[9] HIPC Rule 11(i)(i)
[10] This aspect is inconsistent with the approaches proposed in respect of the TIPC and CRPC, both of which place the IS agency exception alongside other exception clauses.

Unlike the HIPC, there is no express requirement for agencies under the TIPC to have first considered whether authorisation has occurred.

15. The TIPC applies to a very broad range of agencies of varying size and capability, including network operators[11], internet service providers, directory publishers and enquiry agencies, mobile telephone retailers and call centres. Unlike health agencies, the vast majority of these agencies will be private sector organisations who have obtained personal information under a contract for services.

16. The breadth of information defined as a "telecommunications information" under the TIPC (which is inclusive of subscriber information, traffic information and content of a telecommunication) is very broad. However, it is important to note that such information is limited to information about an identifiable individual. The TIPC amendment would therefore not enable telecommunications agencies to disclose to IS agencies any personal information held beyond that which regards an identifiable individual named in a request.

17. Given the implications of the proposed amendment, the Commission would again recommend the development of a TIPC guidance note to assist telecommunications agencies with their decision-making in respect of individual requests. It should emphasise the fact that provision of information to an IS agency is discretionary and is not elevated beyond that of other Rule 11 exceptions. A guidance note could also assist telecommunications agencies in updating their information privacy policies, service contracts and information for consumers to reflect the amendment. Such a guidance note should identify the relevant privacy and human rights considerations, as well as the applicable principles of the UN Guiding Principles on Business and Human Rights

18. The Commission notes that large telecommunications providers will already have considerable knowledge and capability in this area. By way of example we refer to Vodafone's 2015 Law Enforcement Disclosure report which sets out a detailed assessment of the legal and human rights frameworks, governance principles and operating policies and procedures associated with dealing with requests for assistance from law enforcement and IS agencies[12]. If is notable that Vodafone's privacy and law

[11] It is notable that network operators are also subject to the production order regime under Part 3, subpart 2 of the Search and Surveillance Act 2012

[12] https://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html

enforcement principles are strongly affirmative of privacy and human rights standards and include[13]:

- That it [Vodafone] does not allow any access to customer data by any agency or authority unless it is legally required to do so
- That it will not go beyond what is required in the law when responding to demands from agencies for customer data
- That it does not accept any instruction from agencies or authorities that go beyond their jurisdiction or legal mandate
- That it honours international human rights standards to the fullest degree possible
- That it seeks to explain publicly the scope and intent of legal powers available to agencies and authorities

Recommendation 2

That a guidance note on the TIPC IS agency exception under proposed Rule 11(1)(ga) is developed in consultation with affected telecommunications agencies.

The CRPC

19. The amendments proposed for the CRPC have two purposes. The first purpose is substantively the same as the amendments to the HIPC and the TIPC, namely the introduction on exception to the disclosure rule in circumstances where a credit reporter has reasonable grounds to believe that disclosure to an IS agency is necessary to enable the IS agency to perform any of its functions.

20. However, unlike health agencies and telecommunications agencies, proposed Schedule 3A requires IS agencies to co-operate with a credit reporter in respect of compliance checks carried out on any credit information disclosed for this purpose. This provides a greater degree of scrutiny than either the HIPC or TIPC.

21. The second purpose concerns disclosures under access agreements between credit reporters and IS agencies to enable security clearance assessments under s 220 of the Intelligence and Security Act 2017.[14]

[13] ibid

[14] Defined by s220(3) as an assessment conducted by the NZ SIS in the performance of its s 11 functions in making a recommendation as to an individual's suitability to hold a New Zealand Government sponsored national security clearance.

22. The proposed amendments provide that an access agreement is in writing (clause 5) and impose a number of obligations on IS agencies under new Schedule 3A. These include a duty to co-operate with all reasonable compliance checks and systematic reviews carried out by the credit reporter. They also require the IS agencies to take a number of measures to safeguard credit information that they have obtained under an access agreement. These mirror the duties upon credit reporters under Rule 5 of the CRPC and include:

- Written policies and procedures for employees, agents and contractors
- Establishment of controls, including passwords and user identification
- Provision of information and training aimed at ensuring compliance with policies and controls
- Monitoring of usage and compliance with policies and controls
- Taking appropriate action in the event a breach is identified

23. The duties upon IS agencies under the CRPC are more extensive that under the HIPC or TIPC. This is tied to the requirement under the CRPC that credit reporters issue annual assurance reports to the Privacy Commissioner confirming compliance with the law. This aspect of the CRPC reflects the uniquely sensitive nature of credit information, which under clause 5 covers a broad range of information relevant to an individual's financial status and history.

24. However, the proposed amendment does not contain any directive as regards the duties upon the IS agency to either store, or dispose of, an individual's credit information once a security clearance assessment has been made. Given the obligations upon credit reporters under subrule (1) of Rule 5 which reflect the wider public interest as regards the storage and security of credit information, consideration should be given to whether IS agencies ought to be obliged to dispose of any credit information obtained under an access agreement for the purposes of a security clearance assessment once the assessment has been completed.

25. There is no clear public interest basis for enabling IS agencies to hold on to an individual's credit information indefinitely if obtained under an access agreement. Rule 9(1) of the CRPC currently provides that credit reporters may not hold credit information for any longer than is required for the purposes for which the information may lawfully be used. It follows that IS agencies who obtain credit information from a credit reporter for the purpose of undertaking a security clearance should be held to the same standard.

26. The Commission therefore recommends that new Schedule 3A is amended to include a requirement that IS agencies dispose of credit information obtained under an access agreement once the security clearance has been completed. Confirmation of disposal could then be verified by a credit reporter as part of its compliance checks under Schedule 3A.

Recommendation 3

That proposed Schedule 3A of the CRPC is amended to include a requirement that IS agencies dispose of an individual's credit information obtained under an access agreement once the security clearance of that individual has been completed.